

TRABAJO ESPECIAL DE GRADO

RED INALÁMBRICA PARA APLICACIONES EN SISTEMAS DE SEGURIDAD

Presentado ante la Ilustre
Universidad Central de Venezuela
Por el Br. Chávez G. Albert J.
Para optar al título de
Ingeniero Electricista

Caracas, 2006

TRABAJO ESPECIAL DE GRADO

RED INALÁMBRICA PARA APLICACIONES EN SISTEMAS DE SEGURIDAD

TUTOR ACADÉMICO: Ing. José Alonso

Presentado ante la Ilustre
Universidad Central de Venezuela
Por el Br. Chávez G. Albert J.
Para optar al título de
Ingeniero Electricista

Caracas, 2006

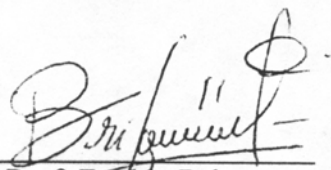
CONSTANCIA DE APROBACIÓN

Caracas 8 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 Albert J. Chávez G., titulado:

“RED INALÁMBRICA PARA APLICACIONES EN SISTEMAS DE SEGURIDAD”

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.

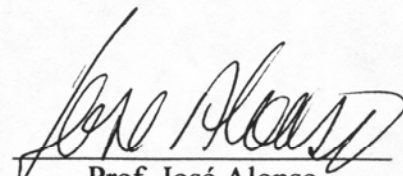

Prof. Freddy Brito

Jurado



Prof. Ebert Brea

Jurado


Prof. José Alonso

Tutor Académico



DEDICATORIA

A Dios y a mis padres, por ser mi apoyo incondicional en ésta y en todas las cosas
que deseo lograr con éxito.

RECONOCIMIENTOS Y AGRADECIMIENTOS

- A todos aquellos que laboran y estudian en la Escuela de Ingeniería Eléctrica, por contribuir con buena disposición a favorecer el proceso de desarrollo del trabajo, y en especial a su Director, Freddy Brito, por mantenerse atento al avance del proyecto.
- A mis compañeros del Laboratorio de Desarrollo, donde precisamente se desarrolló la mayor parte del trabajo del presente proyecto, por su invaluable ayuda y colaboración desinteresada.
- A Boris Roa y José Carrasquel, quienes desarrollaron trabajos paralelos sobre el mismo proyecto global, no sólo por haber participado directamente, sino por dejar un ejemplo de verdadera responsabilidad, interés y fiel cumplimiento de sus responsabilidades.
- Al Prof. Ing. José Alonso, no sólo por la excelente tutela sobre el presente trabajo, sino por mostrar siempre un punto de vista práctico y realista en el ejercicio de los aspectos de la ingeniería, lo cual constituyó un aprendizaje muy valioso.

Chávez G., Albert J.

RED INALÁMBRICA PARA APLICACIONES EN SISTEMAS DE SEGURIDAD

Profesor Guía: 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. 89 h.+anexos.

Palabras Claves: Alarma; Comunicaciones; Módulos Electrónicos; Protocolo; Redes; Seguridad; Sistema inalámbrico.

Resumen. El objetivo de este proyecto consiste en desarrollar un prototipo de sistema de seguridad basado en una red inalámbrica para la Escuela de Ingeniería Eléctrica (EIE) de la Universidad Central de Venezuela (UCV). Dicho sistema se basa en una estructura de transferencia de datos vía inalámbrica, y está conformado por un conjunto de módulos especialmente diseñados para prestar servicios relacionados a seguridad y alarma para edificaciones comerciales o educativas de mediano tamaño. Forma parte de dicho sistema un nivel de redes de bajo volumen de datos para sensores y actuadores inalámbricos que operan en la banda de 400 MHz a baja velocidad y están basados en una topología tipo estrella, concebido con criterio de bajo costo. Por otra parte, hay un nivel de red de mayor volumen de datos cuya arquitectura de red se basa en una estructura de árbol de ramales entrelazados, que opera con una mayor velocidad en la banda de 2.4 GHZ, en el cual hay módulos que prestan importantes funciones, como gestión de datos, control de acceso y repetición de información. Los módulos del sistema están basados en microcontroladores. El objeto del presente trabajo es el diseño de estos módulos y su posterior integración en una red prototipo.

ÍNDICE GENERAL

CONSTANCIA DE APROBACIÓN.....	¡Error! Marcador no definido.
DEDICATORIA	iv
RECONOCIMIENTOS Y AGRADECIMIENTOS	v
RESUMEN.....	vi
LISTA DE TABLAS.....	xi
LISTA DE FIGURAS, ILUSTRACIONES O GRÁFICAS	xii
LISTA DE ACRÓNIMOS	xiv
INTRODUCCIÓN	1
ANTECEDENTES Y JUSTIFICACIÓN	2
FACTIBILIDAD.....	3
OBJETIVO GENERAL	4
OBJETIVOS ESPECÍFICOS.....	4
CAPÍTULO I.....	5
ESTADO DEL ARTE DE LOS SISTEMAS DE SEGURIDAD	5
1. Introducción	5
2. Sistemas de seguridad comerciales	5
2.1. Sistema de Seguridad Inalámbrico PowerMax	5
2.2 Sistema de Seguridad Inalámbrico Home Systems XTR200501.....	6
2.3. Sistema de Seguridad Inalámbrico Magellan MG-6060.....	7
2.4. Sistema de Seguridad Inalámbrico Rokonet WaveSYS.....	7
2.5. Sistema de Seguridad Híbrido Power 832	8
2.6. Sistema de Seguridad Híbrido Security Pro 800 NetworX de GE.....	9
2.7. Sistema de Seguridad Híbrido Solution Ultima 880	9
2.8. Sistema de Seguridad Híbrido Digiplex DGP 848.....	10
2.9. Sistema de Seguridad Híbrido Esprit	11
2.10. Sistema de Seguridad Híbrido Ademco Vista-250FBP	11

2.11. Sistema de Seguridad Híbrido Caddx NX de GE	12
2.12. Sistema de Seguridad Híbrido Rokonet ProSYS NX de GE	13
3. Observaciones	13
CAPÍTULO II	16
ESTRUCTURA Y CARACTERÍSTICAS GENERALES DEL SISTEMA DE SEGURIDAD.....	16
1. Selección del medio de comunicación	16
2. Arquitectura del Sistema	17
2.1. Red de nivel superior	17
2.2 Redes de nivel inferior	20
3. Componentes del sistema en la red de nivel superior	21
4. Módulo de comunicaciones seleccionado para los elementos de la red de nivel superior.....	24
5. Estructura de los datos en la red de nivel superior.....	26
5.1. Estructura de paquetes para acciones de control y gestión de red	26
5.2. Estructura de paquetes para manejo de alarmas.....	28
6. Descripción del protocolo en la red de nivel superior.....	31
7. Componentes del sistema en las redes de nivel inferior	35
8. Módulos de comunicación seleccionados para los elementos de la red de nivel inferior.....	37
9. Modulación y codificación en los elementos de la red de nivel inferior	38
10. Estructura de datos en las redes de nivel inferior.....	39
11. Modo de comunicación en las redes de nivel inferior.....	40
12. Redundancia en los elementos de la red	40
13. Compatibilidad con elementos que operan en protocolo MODBUS	41
14. Sistema de pruebas.....	41
CAPÍTULO III	43
ESTRUCTURA Y CARACTERÍSTICAS DEL MÓDULO MAESTRO DE ZONA.....	43
1. El papel del Maestro de Zona en el sistema.....	43

2. Estructura del Modulo Maestro de Zona.....	45
3. Distribución de los registros internos de operación del MZ	48
3.1- Registros de valores de configuración	49
3.2 Registros de manejo de dispositivos sensores.....	52
3.3 Registros de manejo de dispositivos actuadores	54
3.4 Registros de rutas de acceso.....	55
CAPÍTULO IV	57
ESTRUCTURA Y CARACTERÍSTICAS DEL MÓDULO REPETIDOR.....	57
1. El papel del Repetidor en el sistema	57
2. Estructura del Modulo Repetidor	59
3. Distribución de los registros internos de operación del RP	60
3.1 Registros de valores de configuración	61
3.2 Registros de rutas de acceso.....	62
CAPÍTULO V	64
ESTRUCTURA Y CARACTERÍSTICAS DEL MÓDULO DE CONTROL DE ACCESO	64
1. El papel del Control de Acceso en el sistema	64
2. Funcionamiento del módulo CA	66
3. Estructura del módulo CA.....	67
4.1 Registros de valores de configuración	70
4.2 Registros de gestión de usuarios	71
4.3 Registros de Manejo de Rutas de Acceso	73
5. Control Remoto.....	73
CAPÍTULO VI.....	75
ESTRUCTURA Y CARACTERÍSTICAS DE LOS SENSORES Y ACTUADORES DEL SISTEMA.....	75
1.- Módulos Sensores	75
1.1. Módulo de detección de apertura	77
1.4. Módulo de detección de presencia	79
2. Actuador de contacto seco	80

CAPITULO VII	81
PRUEBAS Y VALIDACIÓN DEL SISTEMA.....	81
RECOMENDACIONES	86
CONCLUSIONES	87
BIBLIOGRAFÍAS	90
ANEXOS.....	93

LISTA DE TABLAS

TABLAS

Tabla 1. Tipos de alarmas generadas por el sistema	29
Tabla 2. Información adicional incluida en los paquetes de alarma	30
Tabla 3. Descripción de los campos de la trama usada en las redes de nivel inferior	39
Tabla 4. Modos de configuración para respaldo	41
Tabla 5. Entradas del MZ y usos asignados.....	46
Tabla 6. Registros de valores de configuración para el MZ	52
Tabla 7. Tiempos de realización de las acciones no reprogramables	56
Tabla 8. Entradas del RP y usos asignados	60
Tabla 9. Registros de valores de configuración para el RP.....	62
Tabla 10. Entradas del CA y usos asignados	69
Tabla 11. Bloque de registros de gestión de usuarios	71
Tabla 12. Valores de trabajo a cargar en la memoria EEPROM interna del sensor ...	77
Tabla 13. Valores de trabajo a cargar en la memoria EEPROM interna del actuador	80

LISTA DE FIGURAS, ILUSTRACIONES O GRÁFICAS

FIGURAS, ILUSTRACIONES O GRÁFICAS

Figura 1. Sistema PowerMax	6
Figura 2. Sistema Home Systems XTR200501.....	6
Figura 3. Sistema Magellan MG-6060.....	7
Figura 4. Sistema Rokonet WaveSys.....	8
Figura 5. Sistema Power 832	8
Figura 6. Sistema Security Pro 800 NetworX de GE.....	9
Figura 7. Sistema Solution Ultima 880	10
Figura 8. Sistema Digiplex DGP 848.....	10
Figura 9. Sistema Esprit	11
Figura 10. Sistema Ademco Vista-250FBP	12
Figura 11. Sistema Caddx NX de GE	12
Figura 12. Sistema Rokonet ProSYS NX de GE	13
Figura 13. Estructura de una red tipo árbol de ramales entrelazados de múltiples niveles	18
Figura 14. Estructura de una red tipo estrella	20
Figura 15. Estructura general del sistema	23
Figura 16. Módulo TRF-24G de Laipac Technology Inc.	24
Figura 17. Estructura de datos en la red de nivel superior	26
Figura 18. Diagrama de flujo del programa principal del protocolo de enlace y red .	31
Figura 19. Diagrama de flujo de la rutina para manejo del mensajes salientes en el canal de control	33
Figura 20. Diagrama de flujo de la rutina para manejo del mensajes entrantes en el canal de control	34

Figura 21. Diagrama de flujo de la rutina para manejo del mensajes entrantes en el canal de alarmas	35
Figura 22. Estructura de las redes de nivel inferior	36
Figura 23. Módulos TLPXXXA y RLPXXXA de Laipac Technology Inc.....	37
Figura 24. Estructura de datos en las redes de nivel inferior	39
Figura 25. Modo de comunicación en las redes de nivel inferior (Ta= tiempo pseudo aleatorio)	40
Figura 26. Posición del módulo MZ en la red.....	44
Figura 27. Diagrama de bloques del módulo MZ	45
Figura 28. Mapa de memoria del módulo MZ	49
Figura 29. Estructura de los registros de memoria de manejo de sensores.....	53
Figura 30. Estructura de los registros de memoria de manejo de actuadores	54
Figura 31. Estructura de los registros de memoria de rutas de acceso.....	55
Figura 32. Posición del módulo RP en la red.....	57
Figura 33. Diagrama de bloques del módulo RP	59
Figura 34. Mapa de memoria del módulo RP	61
Figura 35. Estructura y posición en la red del módulo CA.....	65
Figura 36. Diagrama de bloques del módulo CA.....	68
Figura 37. Mapa de memoria del módulo CA.....	70
Figura 38. Diagrama de bloques del control remoto.....	74
Figura 39. Diagrama del bloques de un módulo sensor	76
Figura 40. Posición de los módulos sensores en el sistema	76
Figura 41. Diagrama del bloques de un módulo actuador	80
Figura 42. Sistema prototipo montado en la EIE de la UCV	84

LISTA DE ACRÓNIMOS

CCGR.....	Centro de Control y Gestión de Red
MZ.....	Maestro de Zona
RP.....	Repetidor
CA.....	Control de Acceso
ChC.....	Canal de Control
ChA.....	Canal de Alarmas

INTRODUCCIÓN

Actualmente, el mercado ofrece diversos sistemas electrónicos de seguridad. Algunos de éstos son cableados, lo que requiere mano de obra especializada para realizar las canalizaciones; resultando poco flexibles en cuanto a movilidad, e inseguros con respecto a la integridad de las líneas de comunicación. Otros son inalámbricos, pero la transmisión de datos no es segura y no son flexibles.

Ante esto, se plantea el desarrollo de una red inalámbrica para aplicaciones en sistemas de seguridad que sea muy flexible y transmita los datos con alto grado de seguridad.

Para el desarrollo de este proyecto, se utilizan tecnologías de última generación presentes en el mercado, dado que éste ofrece diversas soluciones específicas que permiten facilitar el desarrollo modular de la red, dando altos niveles de confiabilidad. A partir de esto, se pasa a diseñar módulos integrados con tareas específicas que permiten manejar cada una de las aplicaciones del sistema.

ANTECEDENTES Y JUSTIFICACIÓN

La seguridad de los bienes y herramientas de uso administrativo y académico de la Universidad Central de Venezuela es una de las preocupaciones de quienes estudian y trabajan en esta Institución. Las repercusiones de este problema dejan de ser cuantificables al tomar en cuenta que atenta directa e indirectamente contra la formación de aquellos que cursan sus estudios en esta Institución, además de perjudicar el funcionamiento de la misma.

En vista de estas circunstancias, las autoridades de la Facultad de Ingeniería de la UCV han mostrado un alto grado de compromiso en la solución de este problema, canalizando apoyo financiero a aquellos proyectos factibles que consideren que puedan contribuir y así hacerlo extensivo a otras áreas afectadas de la Institución. Por su parte, en la Escuela de Ingeniería Eléctrica de la UCV se han realizado otros trabajos relacionados con sistemas de seguridad que sirven como antecedentes para el desarrollo de este trabajo¹.

¹ Entre los más recientes:

“Sistema de Seguridad Inalámbrico, programable con auto-Chequeo”. Roberto Zamorano. Caracas, mayo 2003.

“Sistema de Seguridad de Tercera Generación”. Camilo Ortega. Caracas, mayo 2003.

FACTIBILIDAD

En relación a los requerimientos del proyecto con respecto a la adquisición de equipos, materiales, suministros y subvención económica para la construcción del prototipo; éstos fueron cubiertos por la Facultad de Ingeniería de la UCV, a través del Decanato.

Efectivamente se contó con espacio físico en las instalaciones de la Escuela de Ingeniería Eléctrica equipado con computador personal y acceso a Internet para facilitar el trabajo relacionado con este proyecto.

Asimismo, se dispuso de los recursos de Laboratorio tanto de Comunicaciones como de Electrónica para realizar los ensayos, pruebas y puesta a punto de los sistemas a desarrollar en el marco de esta actividad.

OBJETIVO GENERAL

Desarrollar un prototipo de sistema de seguridad basado en una red inalámbrica para la Escuela de Ingeniería Eléctrica (EIE) de la Universidad Central de Venezuela (UCV).

OBJETIVOS ESPECÍFICOS

- Especificar los requerimientos y definir las variables del sistema de seguridad.
- Diseñar la arquitectura de la red inalámbrica de seguridad, atendiendo a los requerimientos y criterios establecidos.
- Seleccionar los módulos para la transmisión de datos, detección de eventualidades, y ejecución de los mecanismos de respuesta.
- Diseñar la interfaz (hardware y software) de interconexión aplicación/transceptor.
- Implantar en el sistema técnicas apropiadas para la transmisión segura de datos generados por el sistema.
- Diseñar una interfaz para el sistema central (hardware y software) que permita la recepción de los datos de toda la red y la transmisión de los datos asociados a la ejecución de los mecanismos de respuesta.
- Realizar las pruebas necesarias para el correcto funcionamiento del sistema.
- Definir las especificaciones de la red y las interfaces, así como la información relacionada con la operación y configuración de los mismos.

CAPÍTULO I

ESTADO DEL ARTE DE LOS SISTEMAS DE SEGURIDAD

1. Introducción

Antes de comenzar con el diseño de un sistema de seguridad es necesario conocer todos los avances que en estos últimos años han tenido otros sistemas y dispositivos orientados al campo de la seguridad. Este proceso permite conocer todas aquellas características o innovaciones presentes en los sistemas disponibles en el mercado, así como aquellos detalles a los que los fabricantes prestan especial atención y las prestaciones que ofrecen en sus productos para hacerlos más eficientes según el ambiente donde van a operar. A continuación se presentan algunos de los sistemas presentes en el mercado actual y algunas de sus características resaltantes.

2. Sistemas de seguridad comerciales

2.1. Sistema de Seguridad Inalámbrico PowerMax

Este sistema maneja 7 módulos bajo el estándar X-10² para proveer servicios de domótica³. Requiere de conexión a la red eléctrica y conexión telefónica. Permite supervisión de hasta 29 zonas inalámbricas y una cableada. Posee 8 códigos de usuario. A través de la colocación de sensores y módulos homologados, permite detectar diversos eventos y puede controlar cargas en viviendas (luces,

² "X10" es el sistema de comunicación que utilizan los productos compatibles para comunicarse entre ellos que permite controlar cargas domésticas (luces, electrodomésticos, sistemas de riego, entre otros), aprovechando para ello la instalación eléctrica existente de 220 o 110 Volts, evitando la instalación de cables.

³ Conjunto de sistemas que automatizan las diferentes instalaciones de una vivienda

electrodomésticos, sistemas de riego, entre otros). La programación se realiza a través de un software bajo ambiente Windows®. Transmite la información codificada utilizando un protocolo propio (ver figura 1).



Figura 1. Sistema PowerMax

2.2 Sistema de Seguridad Inalámbrico Home Systems XTR200501

Este sistema genera alarmas y provee control domótico vía telefónica o teclado, mediante la colocación de hasta 16 módulos X10. Puede manejar hasta 16 zonas de sensores ampliables. Requiere de conexión telefónica y eléctrica (ver figura 2).



Figura 2. Sistema Home Systems XTR200501

2.3. Sistema de Seguridad Inalámbrico Magellan MG-6060

Este sistema permite detectar diversos tipos de eventos mediante sensores inalámbricos homologados. Entre los aspectos más interesantes se destaca que soporta servicios de domótica a través de módulos X10. Puede manejar hasta 16 zonas y memorizar hasta 256 eventos. Permite solicitar asistencia vía telefónica a través de botones de emergencia (ver figura 3).



Figura 3. Sistema Magellan MG-6060

2.4. Sistema de Seguridad Inalámbrico Rokonet WaveSYS

Este sistema opera en las bandas de 868 MHz o 433 MHz. Por su diseño, los receptores de estos equipos ofrecen mayor sensibilidad y rechazo a interferencias. Se han asignado 24 bits para direcciones. Incluye detección de errores en el aire y permite una comunicación a 2400 bps (ver figura 4).



Figura 4. Sistema Rokonet WaveSys

2.5. Sistema de Seguridad Híbrido Power 832

Este sistema permite programar 8 zonas cableadas y 32 zonas inalámbricas. Tiene un máximo 14 salidas programables cableadas. Puede memorizar 128 eventos. Tiene posibilidades de expansión (8 zonas por tarjeta de expansión). Permite control vía telefónica, y puede manejar hasta 32 dispositivos con el control domótico X10 (ver figura 5).



Figura 5. Sistema Power 832

2.6. Sistema de Seguridad Híbrido Security Pro 800 NetworX de GE

Este sistema puede manejar hasta 48 zonas utilizando una expansión cableada y hasta 48 zonas vía inalámbrica. Puede asignarse zonas a una o a múltiples particiones. Maneja un máximo de 24 teclados, posee sirena integrada y puede manejar toda la línea de sensores la familia Security Pro de GE. Memoriza hasta 185 eventos (ver figura 6).



Figura 6. Sistema Security Pro 800 NetworX de GE

2.7. Sistema de Seguridad Híbrido Solution Ultima 880

Se trata de un sistema cableado que incluye como opción un receptor vía radio compatible con elementos inalámbricos (detectores, contactos y mandos). Posee 16 códigos de usuario programables, 8 códigos de usuario por mandos vía radio. Pueden programarse hasta 8 zonas. Posee indicador de fallo de alimentación y sistema de supervisión de sensores. La central posee 4 salidas programables, salida para sirena externa y teclas de alarma (ver figura 7).



Figura 7. Sistema Solution Ultima 880

2.8. Sistema de Seguridad Híbrido Digiplex DGP 848

Puede armarse este sistema de seguridad como una combinación cableada o inalámbrica y expandirse a través de la colocación de módulos sobre un bus de cuatro conductores, los cuales pueden ser asignados a una zona en específico. Puede colocarse una serie de sensores o módulos en el bus directamente o conectarse una interfaz inalámbrica de expansión. Este sistema puede manejar hasta 48 zonas bajo 8 particiones. Tiene 96 códigos de acceso, puede memorizar hasta 1024 eventos y soporta hasta 95 módulos de expansión (ver figura 8).

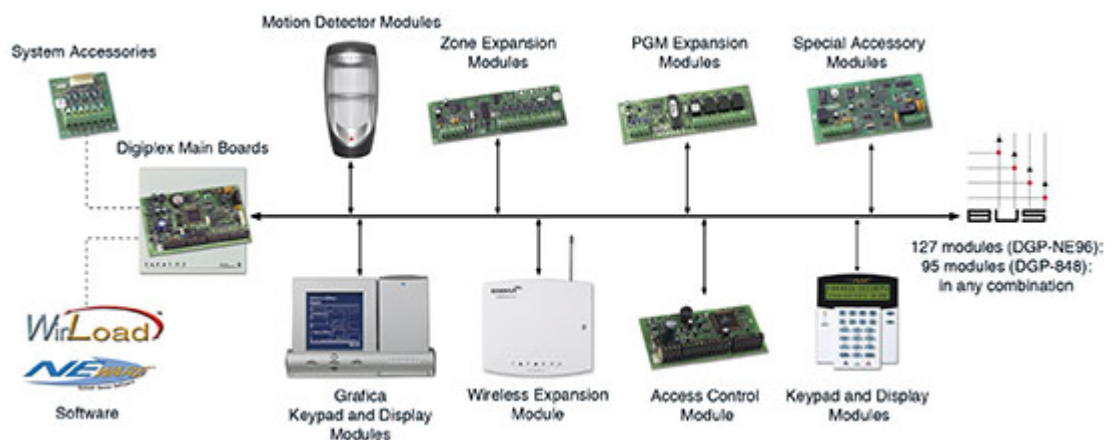


Figura 8. Sistema Digiplex DGP 848

2.9. Sistema de Seguridad Híbrido Esprit

Esta línea de sistemas permite incorporar una amplia gama de centrales con 4, 6 o 12 terminales de entrada de zona y acepta hasta 2 zonas por consola de teclado. Todas estas centrales ofrecen la función de “doblado de zonas” que permite conectar dos dispositivos de detección a un terminal de entrada. Cada dispositivo de detección ocupa su propia zona y comunica su estado a la central. De acuerdo a la central, el sistema puede contar con hasta 24 zonas programables que pueden ser asignadas a una o ambas particiones o a ninguna partición para formar un área común. Permite memorizar hasta 256 eventos. Tiene 49 códigos de usuario (ver figura 9).

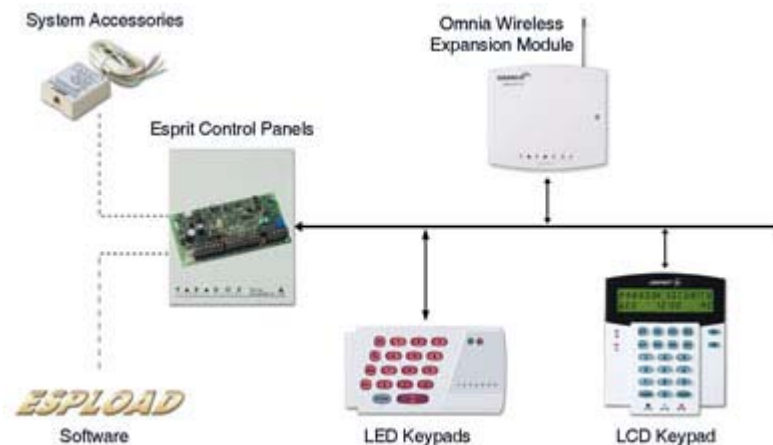


Figura 9. Sistema Esprit

2.10. Sistema de Seguridad Híbrido Ademco Vista-250FBP

Este sistema soporta 8 zonas cableadas expandibles hasta 242 puntos adicionales cableados o 250 puntos inalámbricos. Puede controlar hasta 8 áreas independientes. Puede colocársele sensores comerciales inalámbricos certificados bajo UL. Permite almacenar hasta 1000 eventos y 250 códigos de usuario. Soporta

aplicaciones de CCTV. Soporta control remoto vía Internet y consolas de representación gráfica. Puede manejar hasta 32 controles de acceso (ver figura 10).



Figura 10. Sistema Ademco Vista-250FBP

2.11. Sistema de Seguridad Híbrido Caddx NX de GE

Este sistema puede expandirse a 192 zonas alambradas o inalámbricas. Soporta 240 códigos de usuario, y puede memorizar hasta 512 eventos, manejando 8 zonas de forma independiente. Posee verificación para evitar falsas alarmas y determina el nivel de la batería (ver figura 11).



Figura 11. Sistema Caddx NX de GE

2.12. Sistema de Seguridad Híbrido Rokonet ProSYS NX de GE

Este sistema soporta entre 8 y 128 zonas de monitoreo en hasta 8 particiones, y hasta 16 controles de acceso. Permite expansión inalámbrica e incorporación del estándar X10. También incluye un módulo de voz interactivo (ver figura 12).

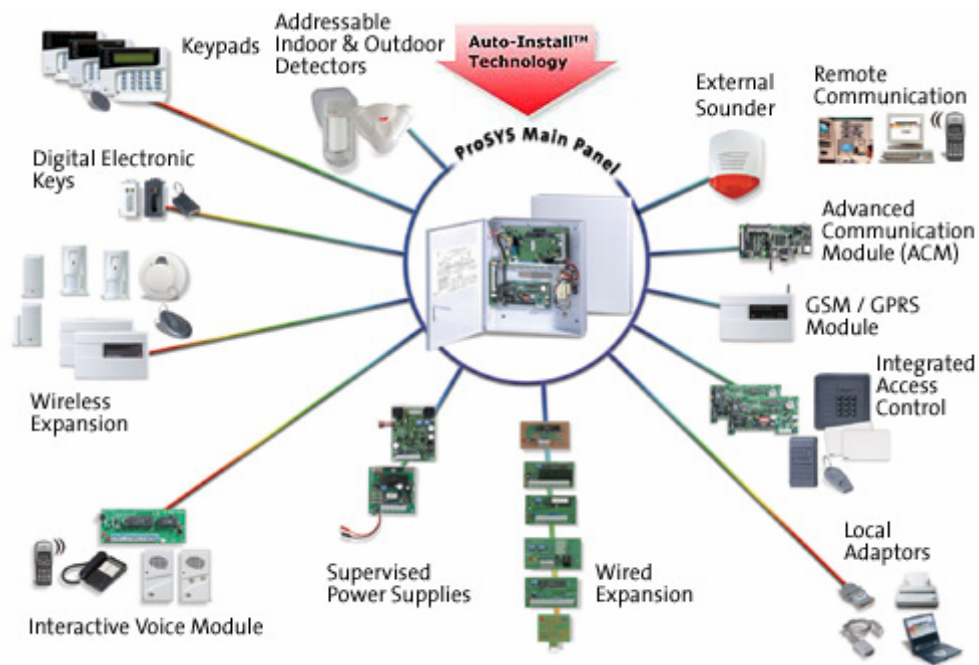


Figura 12. Sistema Rokonet ProSYS NX de GE

3. Observaciones

Muchos de los sistemas disponibles en el mercado están dirigidos a instalaciones domésticas. La mayoría de éstos pueden detectar humo, gas, presencia de intrusos, apertura de puertas o ruptura de ventanas, y adicionalmente ofrecen prestaciones asociadas con el control de cargas en vivienda (domótica) a través del sistema de control X10, el cual permite controlar el encendido y apagado de diversas cargas en viviendas.

Dado que una vivienda promedio no tiene un área demasiado grande en comparación con edificios comerciales o educativos, suelen usarse sistemas inalámbricos con arquitectura en estrella de baja potencia, lo que obliga a la central a estar aproximadamente en el centro geométrico de la edificación, lo cual es una limitante importante. En estos sistemas se usan sensores y actuadores inalámbricos los cuales transmiten vía radiofrecuencia la información de los eventos a la central. Usualmente, cada módulo está conformado por un solo sensor o actuador, batería y módulo de comunicaciones. La comunicación entre los módulos y la central se realiza según un “protocolo propietario” en la mayoría de los casos, lo cual obliga al cliente a comprar sensores y actuadores homologados. Los sensores suelen ser relativamente más costosos comparados con los de los sistemas cableados.

Por su parte, una cantidad importante de sistemas de seguridad comercial que prestan mayores prestaciones suelen ser cableados, es decir, están conformados por una central y un número limitado de módulos sensores y actuadores cableados a la central, la cual es el controlador principal de todo el sistema. La mayoría opera bajo un sistema de comunicaciones de “protocolo y código propietario”, lo que hace en muchos casos que sólo los módulos ofrecidos por el fabricante sean compatibles al sistema. Dentro de esta clasificación, se pueden encontrar dos tipos, los pasivos y los activos. En los sistemas de cableado pasivo, los módulos están conectados individualmente a la central, es decir hay al menos un par de cables por cada módulo. Esto hace que el número de cables que conforman el sistema sea muy numeroso, lo que dificulta la instalación. Este tipo de sistema prácticamente está desapareciendo del mercado. Los sistemas de cableado activo están conformados por un bus de comunicación serial donde se emplea un protocolo. Por tal razón, cada módulo debe estar conformado por un sensor o actuador y un puerto de comunicaciones. Una de las desventajas de esta topología es que una falla en el bus inhabilita gran parte del sistema.

Los sistemas cableados pueden ser rentables en aquellos proyectos planificados de construcción y remodelación de áreas comerciales o educativas, pero son costosos y muy complicados de canalizar en edificaciones ya terminadas y amobladas. En la investigación que se realizó, no se encontraron fabricantes que ofrecieran sistemas completamente inalámbricos para aplicaciones no residenciales.

Muchos fabricantes, por competitividad, han incorporado módulos inalámbricos a modo de expansión a estos buses o redes cableadas, lo cual permite controlar un número determinado de terminales. Esta tendencia se ha hecho común, y ha producido una generación de sistemas mixtos o híbridos. Estos sistemas están conformados por una combinación entre los sistemas inalámbricos y los sistemas cableados. Algunos de estos manejan una comunicación inalámbrica con los sensores y una comunicación cableada aparte con los actuadores. En la gran parte de los sistemas híbridos la parte cableada es del tipo activo.

En general, los fabricantes consideran importantes en los sistemas que ofrecen ciertas características tales como el número de zonas que se pueden supervisar, el número de sensores y actuadores que soportan, la cantidad de eventos y códigos de usuario que se pueden almacenar, la posibilidad de control remoto (control telefónico, mando a distancia o control a través de Internet, entre otros), la capacidad de detección de falsas alarmas y la determinación del nivel de batería. A fin de hacer el producto más atractivo para el cliente, se suele incorporar la capacidad de control de cargas.

Todas estas características anteriormente expuestas se toman en cuenta en el presente trabajo con la intención de tomarlas como punto de partida en el proceso de diseño, a fin no sólo incorporar algunas de ellas, si mejorarlas en algunos aspectos.

CAPÍTULO II

ESTRUCTURA Y CARACTERÍSTICAS GENERALES DEL SISTEMA DE SEGURIDAD

1. Selección del medio de comunicación

Generalmente, la instalación de sistemas cableados requiere de obras de canalización en edificios terminados, lo cual incrementa sensiblemente los costos. En algunas instalaciones se suele dejar cables o canaletas a la vista, lo cual es indeseable en un edificio como la EIE de la UCV, ya que aparte de perjudicar la apariencia de la arquitectura del edificio, no ofrece el nivel de seguridad sobre la integridad del sistema que se requeriría. Esa es la razón más importante por la que se ha optado por un sistema completamente inalámbrico. Entre las ventajas más importantes de este tipo de sistema, se puede destacar el hecho de que ofrece mayor nivel de seguridad tanto de la integridad propia del sistema como en la información que viaja en él, y su instalación es mucho más fácil y rápida que en el caso de los sistemas cableados.

Como ya se ha mencionado, muchos de los sistemas de seguridad inalámbricos poseen módulos que están conformados por un solo sensor o actuador, batería y módulo de comunicaciones. Los sensores suelen ser relativamente más costosos comparados con los de los sistemas cableados. La topología más usada en este tipo de sistemas (generalmente para ser utilizados en residencias unifamiliares) es la de estrella, lo que obliga a la central a estar aproximadamente en el centro geométrico de la edificación, con un alcance circular, lo cual es una limitante importante. A fin de solucionar esta limitante, se ha pensado en una arquitectura de múltiples niveles de características particulares, la cual se plantea a continuación.

2. Arquitectura del Sistema

En general, las dimensiones de un edificio del tipo educativo usualmente son mucho mayores que en el caso de las viviendas unifamiliares, y muy rara vez presentan una arquitectura de simetría radial. Por tal razón, no es apropiado diseñar el sistema que se plantea basándolo en una red tipo estrella.

A fin de estructurar el sistema desde un punto de vista práctico y con criterio de bajo costo, se han definido claramente dos niveles de red, una red denominada red de nivel superior y un conjunto de redes denominadas redes de nivel inferior.

2.1. Red de nivel superior

La red de nivel superior está conformada por los elementos que manejan mayor volumen de datos. Luego de considerar diversos tipos de topologías⁴ tomando diversos criterios como los costos, la dificultad de programación, las limitaciones del hardware y los retardos en la transmisión de datos, se tomó la decisión de basar la arquitectura de la red de nivel superior bajo una estructura de árbol de ramales entrelazados de múltiples niveles. En esta topología, el árbol tiene su primer nodo en la raíz y se expande a través de ramas, en donde se conectan las demás terminales (ver figura 13).

En la arquitectura seleccionada es posible albergar un número de componentes más elevado y puede ampliarse la red agregando más nodos. Esto hace al sistema más robusto, dado que si falla un nodo, el tráfico puede distribuirse hacia los demás. Adicionalmente, los nuevos componentes recién instalados pueden irse conectando a las zonas menos congestionadas. Esta topología soluciona el problema del alcance de algunos componentes muy alejados. La administración del sistema puede ser distribuida o centralizada, interpretándose como un componente más del

⁴ Como topologías en estrella, bus, anillo o malla.

sistema y ubicado físicamente en alguno de los nodos. En el caso de este sistema, la administración de la red es centralizada y la realiza el módulo CCGR (Centro de Control y Gestión de Red), el cual está físicamente ubicado en el centro de la red (nodo raíz).

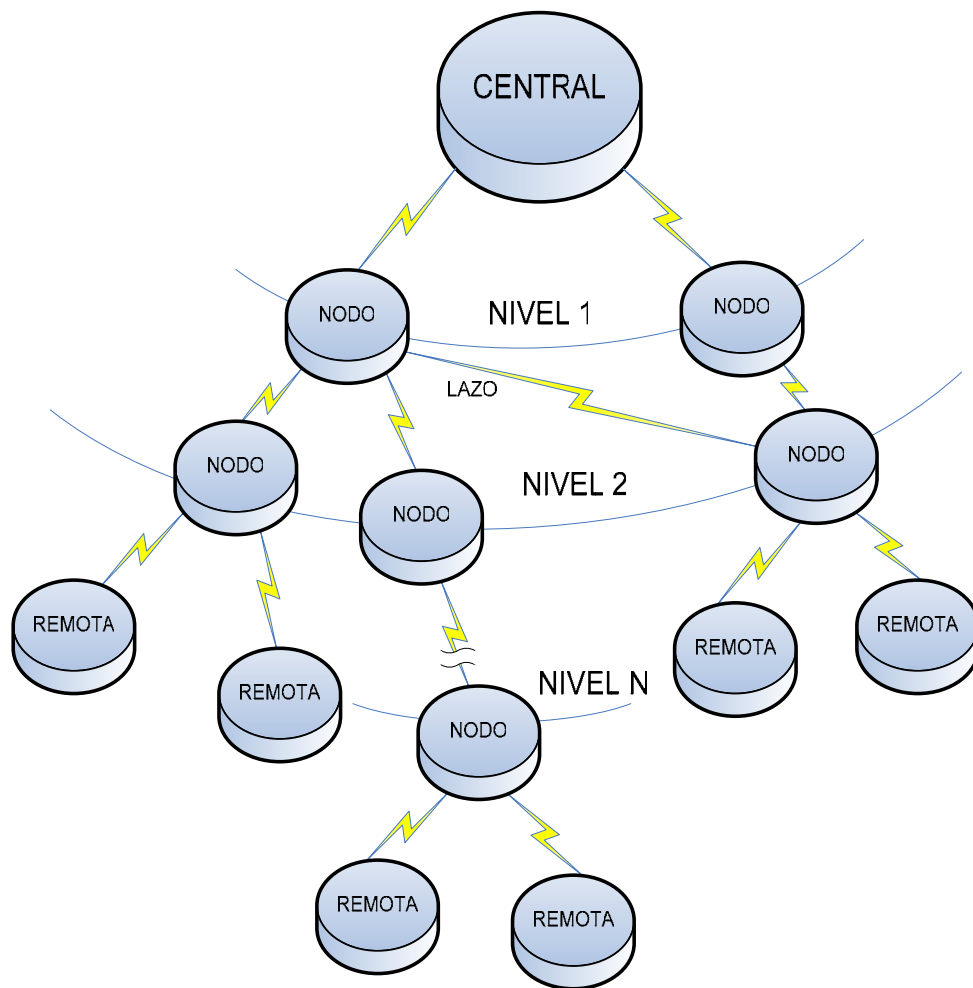


Figura 13. Estructura de una red tipo árbol de ramales entrelazados de múltiples niveles

Este tipo de redes puede tener diversos grados de interconexión entre los nodos. De hecho, en la red que se plantea en el presente trabajo, algunos nodos de diversos ramales y niveles están entrelazados, por lo cual las rutas han de

programarse cuidadosamente para evitar lazos donde los paquetes se pierdan. La configuración de la red se hace por niveles.

En la red de nivel superior se ha definido un máximo de 247 elementos⁵. Adicionalmente, para evitar retardos muy prolongados en la transferencia de información desde el punto donde se genera el evento hasta el módulo central, se ha limitado el número de repetidores a 8 por ruta (8 niveles). La red de nivel superior opera en dos canales de forma simultánea; un canal denominado canal de control en el cual viaja la información asociada al funcionamiento de la red como tal y un canal de alarmas en el cual viaja la información asociada a las alarmas que se generan debido a los eventos que detecta el sistema. Todas las comunicaciones en el sistema se realizan en modo punto a punto, en el cual un dispositivo envía un mensaje sólo a un receptor.

En virtud de que el sistema opera empleando 2 canales de frecuencia en la red de nivel superior y hay 125 canales de frecuencia disponibles en esa banda (ISM de 2.4 GHz) para los módulos transceptores empleados⁶; en caso de ser necesario un sistema de mayores dimensiones, es posible integrar hasta 62 redes similares (todas con centrales separadas). De cualquier manera, no resultaría práctico para un operador monitorear y manejar más terminales de las que soporta una red⁷ desde un monitor único, y además el CCGR se congestionaría tratando de manejar una red demasiado grande reduciendo la velocidad del sistema.

⁵ Incluyendo nodos y terminales

⁶ La descripción de estos módulos se presenta en la sección 4 de este mismo capítulo.

⁷ Según las características que se plantean en el presente trabajo.

2.2 Redes de nivel inferior

Las redes de nivel inferior son subredes de la red de nivel superior y operan en la banda de frecuencia de 400 MHz. Dichas redes están conformadas por los dispositivos sensores y actuadores inalámbricos.

La estructura de una red de nivel inferior es de estrella centralizada alrededor de un módulo terminal de la red de nivel superior. En una red tipo estrella, todos los componentes están conectados directamente con el administrador central, formando una figura de una estrella con múltiples brazos: uno por componente instalado (ver figura 14).

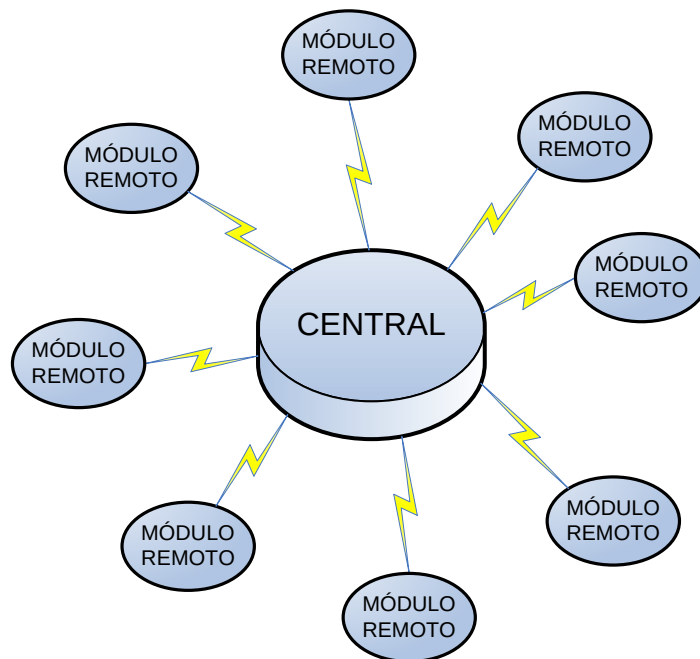


Figura 14. Estructura de una red tipo estrella

La estructura de estrella es la más apropiada dado que los dispositivos sensores y actuadores tienen un patrón de radiación isotrópico debido a que la antena

que se le coloca es del tipo dipolo vertical de un cuarto de la longitud de onda. Adicionalmente, esta topología permite que los sensores y actuadores se distribuyan alrededor del elemento que recoge los datos sin necesidad de orientar las antenas.

3. Componentes del sistema en la red de nivel superior

La red de nivel superior está compuesta por tres tipos de módulos⁸, a saber:

- **Módulos Maestro de Zona (MZ):** Su función es recoger la información desde los sensores inalámbricos, y procesar esa información para hacerla llegar hasta el CCGR⁹; así como recibir información desde el CCGR para activar o desactivar módulos actuadores inalámbricos. El MZ actúa como una central que recoge los datos provenientes de los elementos que están en la red de nivel inferior y empaqueta esa información para elevarla a la red de nivel superior. Cada MZ puede manejar un máximo de 64 sensores inalámbricos y 64 actuadores inalámbricos. Se ha limitado el número de terminales para no congestionar el canal de la red de nivel inferior debido a colisiones y exceso de información en el aire, ya que cada MZ puede manejar solamente un canal para sensores y uno para actuadores.
- **Módulos de Control de Acceso (CA):** Su función es gestionar la salida y entrada de usuarios a determinados espacios controlados y reportar las alarmas asociadas a dicha gestión procesando la información para enviarla al CCGR.
- **Módulos Repetidores (RP):** Su función es repetir y enrutar la información proveniente de otros dispositivos.

⁸ En los capítulos 3, 4 y 5 se describen individualmente con mucho más detalle.

⁹ En este trabajo no se contempla el diseño del CCGR.

Toda la información que viaja a través de la red de nivel superior converge al CCGR, un módulo diseñado para recoger las alarmas que genera toda la red, manejar los registros internos de todos los módulos para su correcto funcionamiento, gestionar y almacenar las alarmas y sus secuencias y transmitir los datos hacia un computador personal (PC). Dicho PC organiza la información asociada a la red para facilitar su administración, respalda los datos en memoria local y hace disponible a otros monitores a través de una red un acceso limitado a otros usuarios que monitorean el sistema. La figura 15 describe la estructura general del sistema.

Para obtener más información sobre el CCGR, véase el Trabajo de Grado “Sistema de Control Maestro para el Sistema de Seguridad Inalámbrico de la EIE de la UCV”, presentado por el Br. José Carrasquel.

Cabe destacar que todos los parámetros de funcionamiento de los elementos de la red de nivel superior (MZ, CA, RP) son configurables de forma remota. Adicionalmente, todos los módulos de la red de nivel superior cuentan con batería y transformador, el cual permite recargar la batería mientras esté conectado. Todos los elementos de este nivel pueden detectar el nivel de la batería y la presencia del transformador. El uso de batería es una ventaja, por cuanto puede sostener a los elementos sistema por un tiempo de autonomía que depende del número de eventos que se genere y de algunos parámetros dinámicos de configuración¹⁰.

Todos los módulos de la red de nivel superior se basan en microcontroladores de la familia PIC18 de MICROCHIP, y fueron programados en lenguaje C sobre el compilador PICC18 versión de evaluación 8.35PL3 de HI-TECH en ambiente MPLAB IDE v7.30 de MICROCHIP.

¹⁰ La determinación del tiempo de autonomía de cada módulo implica pruebas de mayor extensión temporal, lo cual no podría hacerse sin retrasar el curso de este trabajo.

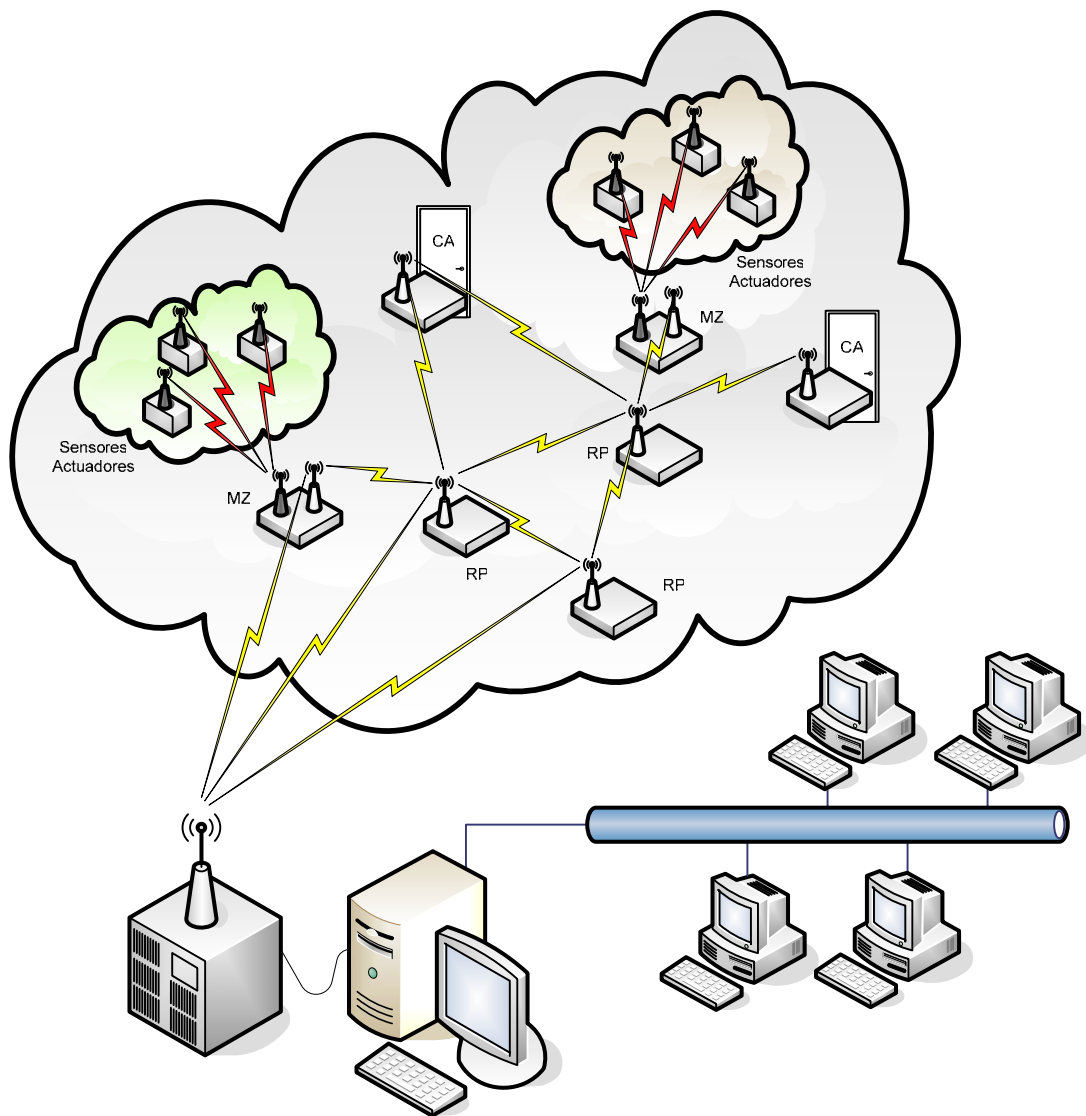


Figura 15. Estructura general del sistema

4. Módulo de comunicaciones seleccionado para los elementos de la red de nivel superior

Los transceptores que se han seleccionado para interconectar los elementos de la red nivel superior de forma inalámbrica son los módulos TRF-24G de Laipac Technologies Inc (ver figura 16).

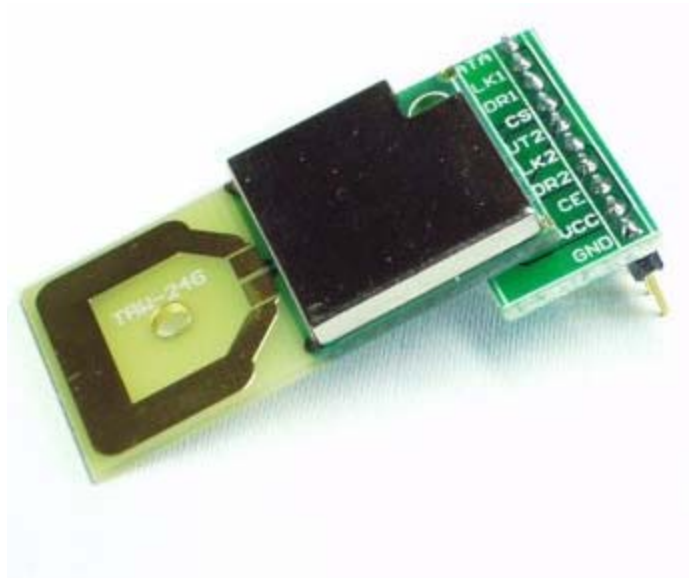


Figura 16. Módulo TRF-24G de Laipac Technology Inc.

Los módulos TRF-24G poseen las siguientes características básicas:

- Rango de Frecuencia entre 2.400 ~ 2.524 GHz en la banda ISM¹¹
- Modulación GFSK¹²
- Velocidad de transmisión de hasta 1Mbps
- 125 canales disponibles
- Receptor doble simultáneo

¹¹ Industrial Science Medical

¹² Gaussian Frequency Shift Keying (FSK con filtro gaussiano)

- Incluye decodificador, codificador, buffer de datos y cálculo de CRC
- Modo ShockBurst para ahorro de energía
- Sensibilidad de -90 dBm
- Antena incorporada
- Tamaño reducido (20.5mm x 36.5mm x 2.4mm)
- Costo razonable¹³

Las características del módulo TRF-24G lo hacen muy apropiado para aplicaciones de transmisión inalámbrica de datos en sistemas de seguridad. Sin embargo, por las características de la antena que posee, la cual es altamente direccional, los dispositivos requieren orientación para lograr el enlace. La velocidad a la que funciona la transmisión de datos se ha programado en 250.000 bps, lo cual aumenta la sensibilidad en la recepción en 10 dB.

En la red de nivel superior se utiliza la modalidad de doble receptor simultáneo (en la cual el transceptor puede recibir datos en dos canales separados al mismo tiempo). Esto es lo que permite al CCGR manejar un canal independiente para acciones de control sobre los elementos del sistema (configuración de dispositivos y solicitud de datos) y un canal diferente para alarmas.

¹³ \$19 por unidad para el año 2006

5. Estructura de los datos en la red de nivel superior

5.1. Estructura de paquetes para acciones de control y gestión de red

En la red de nivel superior la estructura de la trama es la que puede observarse en la figura 17. Estos paquetes son transmitidos a través del canal de control.

Preámbulo	DE	DR	DD	TT	25 Bytes de Datos	CRC LOW	CRC HIGH
-----------	----	----	----	----	-------------------	---------	----------

Figura 17. Estructura de datos en la red de nivel superior

El preámbulo es un espacio de 4 bits el cual es empleado por el dispositivo transceptor para sincronizar el paquete.

Tal como puede observarse en la figura 17, los bytes DE, DR, DD, TT ,CRC LOW y CRC HIGH en la trama son específicamente utilizados para direccionamiento y manejo de la misma, y forman parte de un protocolo propietario denominado “EIEUCV2006V1” de la capa de enlace del sistema de comunicaciones. Las funciones de dichos campos son las siguientes:

- DE (Dirección de envío): Es un byte en el cual se coloca la dirección del dispositivo inmediato hacia la cual la trama es enviada.
- DR (Dirección de Respuesta): Es un byte en el cual el dispositivo que envía la trama coloca su dirección propia, para que el dispositivo receptor conozca de donde proviene la trama y pueda generar una respuesta.
- DD (Dirección de Destino): Es un byte que contiene la dirección del dispositivo final al cual va dirigido el mensaje.

- TT (Tipo de Trama): Es un byte que contiene un código que indica la acción inmediata que el dispositivo receptor debe realizar con la trama.
- CRC LOW y CRC HIGH: Estos bytes contienen el Código de Redundancia Cíclica de 16 bits, un código de verificación de errores. El campo CRC es un valor binario de 16 bits. El valor CRC es calculado por el dispositivo emisor, que lo añade al mensaje. El dispositivo receptor calcula el CRC durante la recepción del mensaje y compara el valor calculado con el valor recibido en el campo CRC LOW y CRC HIGH. Si los dos valores no son iguales, resulta un error. En este caso, el CRC es calculado sobre toda la trama a partir del campo DR, ya que el dispositivo que recibe la trama elimina el campo DE.

Hay cuatro códigos de tipo de trama (TT) empleados en el canal de control, a saber:

- 01 (Repetición): El mensaje recibido es para ser repetido hacia otro dispositivo para lograr el acceso hacia el dispositivo de destino, si dicha dirección es diferente a la propia.
- 02 (Control): El mensaje recibido es para ser procesado localmente, ya que se trata de una trama que contiene una solicitud o configuración proveniente del CCGR, si la dirección de destino es la propia del dispositivo en cuestión.
- 03 (Confirmación): El mensaje es una confirmación que contiene una copia del mensaje recibido.
- 04 (Falla en la red): El mensaje contiene una alarma asociada a una falla en el sistema de comunicaciones debido a que no se logró establecer un enlace específico.

Dentro de los 25 bytes de datos destinados para la capa de red, está el paquete que contiene la información asociada a las funciones de configuración y notificación de alarmas según una estructura multimaestro. Esto es válido tanto para el canal de alarmas como para el canal de control.

5.2. Estructura de paquetes para manejo de alarmas

El manejo de alarmas (sobre el canal de alarmas) está constituido por la misma capa física y los mismos protocolos de enlace y de red usados para la parte de control y gestión de red en el canal de control. Aunque el uso de los campos DD, DE y DR de la capa de enlace del canal de alarmas es idéntico al uso que se les da en el canal de control (de acuerdo a la figura 17), en el canal de alarmas sólo se maneja el Tipo de Trama (TT) número 05. Un mensaje con este tipo de trama contiene información asociada a una alarma del sistema, las cuales provienen de eventos asociados directamente a las acciones de seguridad.

Ambos tipos de mensajes pueden ser entrantes o salientes. De cualquier modo, son repetidos o enviados hacia el CCGR. En el campo destinado para datos, puede viajar alguna de las alarmas listadas en la tabla 1.

Tabla 1. Tipos de alarmas generadas por el sistema

Tipo de alarma	Fuente de la alarma	Descripción
01	Entrada local	Se ha activado una entrada local.
02	Falla de enlace	Un equipo que provee una ruta de acceso para llegar a un elemento terminal no respondió.
03	Dispositivo no se reporta	Un elemento de la red no respondió al barrido de verificación de integridad o un sensor no se reportó
04	Sensor inalámbrico detecta evento	Un sensor inalámbrico detectó un evento
05	Rutas agotadas	No fue posible acceder a un equipo terminal y no hay más rutas de acceso programadas
06	Dispositivo violentado	Ha sido activada la entrada de autoprotección de un equipo de la red
07	Desconexión de línea	Se ha desconectado el transformador de una terminal de la red
08	Acceso entrada	Un usuario ha accedido a un espacio controlado usando su control
09	Acceso salida	Un usuario ha salido de un espacio controlado usando su control
10	Acceso denegado	Alguien ha tratado de ingresar sin éxito a un espacio controlado. Ha ingresado la clave de forma incorrecta más de tres veces.
11	Usuario en pánico	Un usuario ha accedido a un espacio controlado usando su clave de pánico
12	Nuevo sensor detectado	Se ha encendido un sensor inalámbrico nuevo y no se ha configurado en la red

Con las alarmas provenientes de la red, se adjunta información adicional que permite al CCGR determinar de dónde se genera la alarma o la causa que la origina (ver tabla 2).

Tabla 2. Información adicional incluida en los paquetes de alarma

Tipo de alarma	Información adicional adjuntada
01	Dirección del equipo que generó la alarma y de la entrada activada
02	Dirección del equipo que generó la alarma y del equipo que no proveyó la ruta de acceso
03	Dirección del equipo que generó la alarma y del equipo o sensor que no se reportó
04	Dirección del equipo que generó la alarma, del sensor que reportó el evento y zona de donde proviene
05	Dirección del equipo que generó la alarma y del equipo al que no se pudo acceder a través de alguna ruta.
06	Dirección del equipo o sensor violentado
07	Dirección del equipo
08	Dirección del CA que generó la alarma y número del usuario
09	Dirección del CA que generó la alarma y número del usuario
10	Dirección del CA que generó la alarma y número del usuario
11	Dirección del CA que generó la alarma y número del usuario
12	Número del sensor que se ha encendido y zona de donde proviene

La estructura de datos de manejo de alarmas permite incorporar al sistema más fuentes de alarma para aumentar la capacidad del sistema.

6. Descripción del protocolo en la red de nivel superior

El funcionamiento del protocolo está descrito en forma resumida en los diagramas de flujo que se presentan a continuación, los cuales presentan los algoritmos que han sido programados en todos los equipos.

Dentro del programa principal, la unidad central de proceso de todos los dispositivos verifica si hay mensajes salientes (generados por eventos locales) o si se han presentado mensajes entrantes en cualquiera de los dos canales (canal de control o canal de alarmas). Si se presenta un mensaje saliente, se ejecuta la rutina para elaborar y manejar el mensaje saliente de acuerdo a la estructura y el protocolo. Por otra parte, si se ha presentado un mensaje entrante, éste será procesado dependiendo del canal por el cual se recibe y el tipo de tarea que se solicite (ver figura 18).

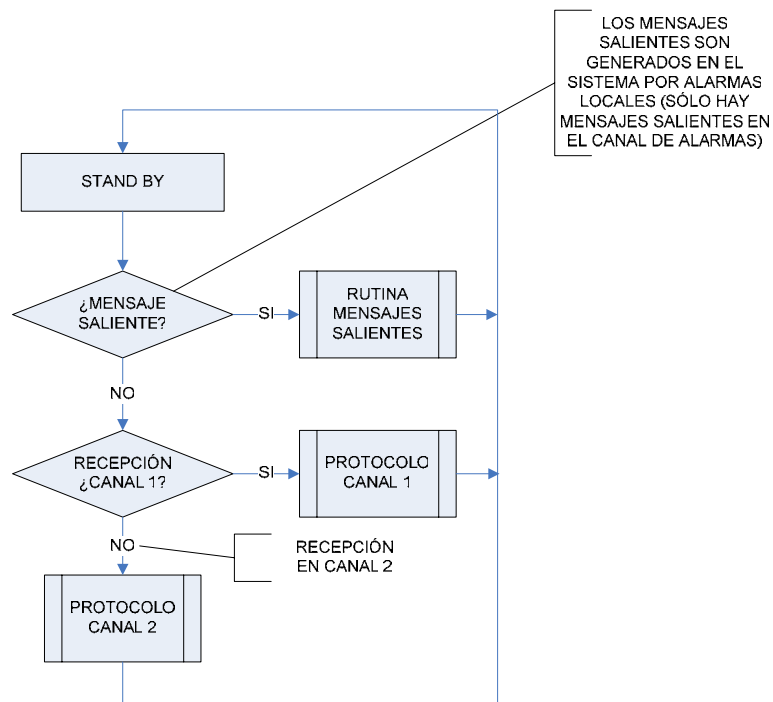


Figura 18. Diagrama de flujo del programa principal del protocolo de enlace y red

En la rutina para manejo de los mensajes salientes en el canal de control, primero se revisa una tabla de rutas interna en busca de una ruta hacia el dispositivo destino. Si existe una ruta, se toma y se empaqueta el mensaje según la estructura anteriormente explicada. El dispositivo queda en recepción, esperando durante un tiempo configurado por una confirmación del receptor. De llegar la confirmación, eso implica que mensaje ha sido entregado con éxito y la rutina termina. De lo contrario, el mensaje se repetirá un número determinado de veces esperando hasta obtener una confirmación. Si esto no ocurre después de todos los intentos, se pasa a buscar otra ruta y el proceso se repite. De no haber otra ruta, eso implica que no hay manera de acceder al CCGR y por lo tanto la rutina termina (ver figura 19).

Si ha llegado un mensaje por el canal de control, se ejecuta la rutina “Protocolo Canal 1”. En esta rutina se almacenan en variables temporales los campos que conforman la cabecera del paquete, a saber DD, DR y TT; los cuales servirán para configurar los mensajes salientes. Si el mensaje recibido es una solicitud de repetición ($TT=1$), se confirma la recepción de dicho mensaje al elemento que lo envió (cuya dirección es DR) y se pasa a la rutina de repetición (esta rutina sólo puede ser procesada por el dispositivo repetidor RP). Por otro lado, si el mensaje es de control, se verifica que la dirección sea la propia para confirmar al elemento que lo envió y se ejecuta la rutina de mensajes de control, la cual pueden ejecutar todos los dispositivos de la red de nivel superior (CA, MZ y RP). Si el mensaje recibido es de falla ($TT=4$), se verifica que vaya dirigido al CCGR y luego se confirma la recepción de dicho mensaje al elemento que lo envió (cuya dirección es DR) y se pasa a la rutina de mensajes salientes en el canal de control (en la cual se realizará el proceso de entrega hacia el CCGR) (ver figura 20).

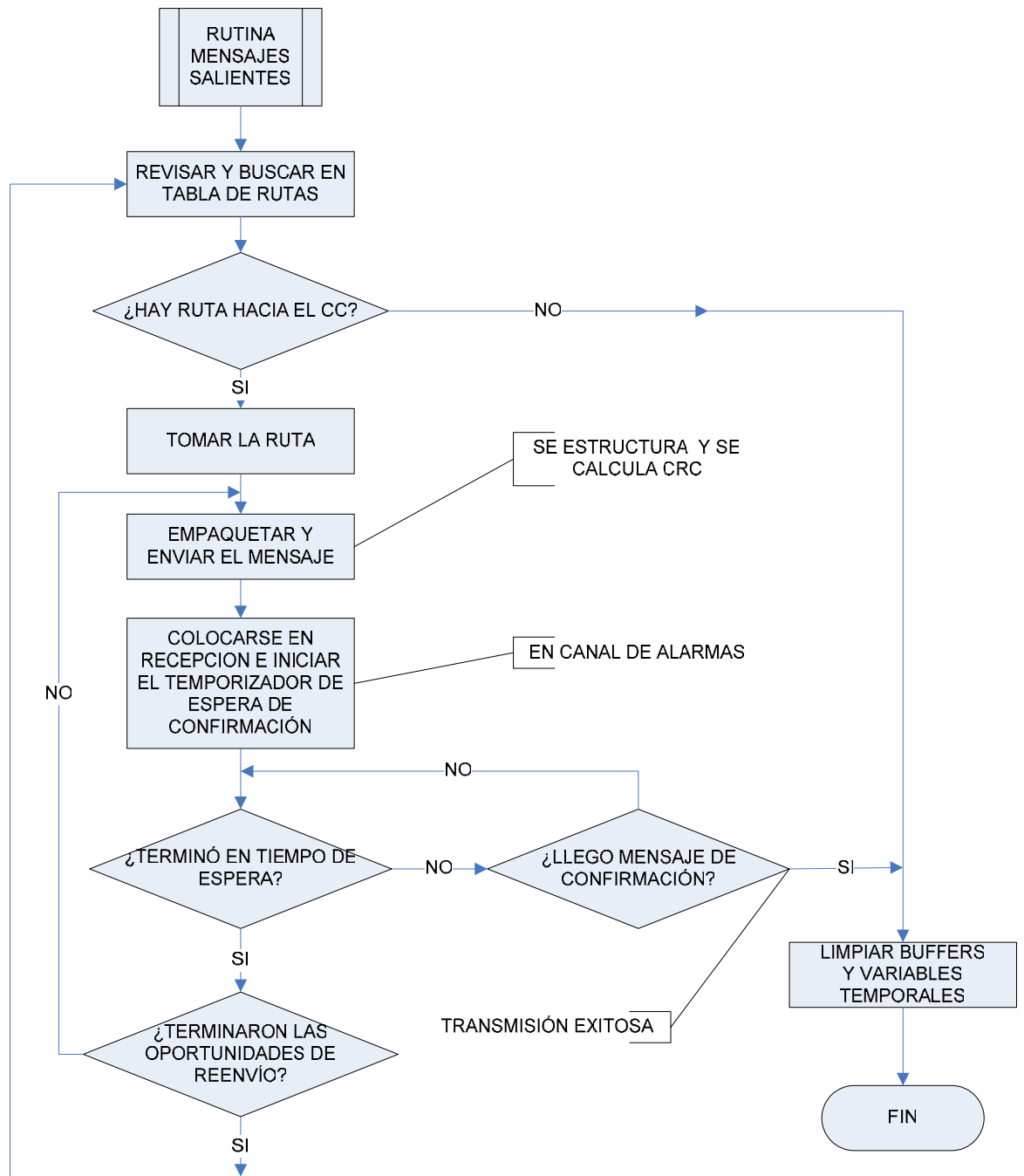


Figura 19. Diagrama de flujo de la rutina para manejo del mensajes salientes en el canal de control

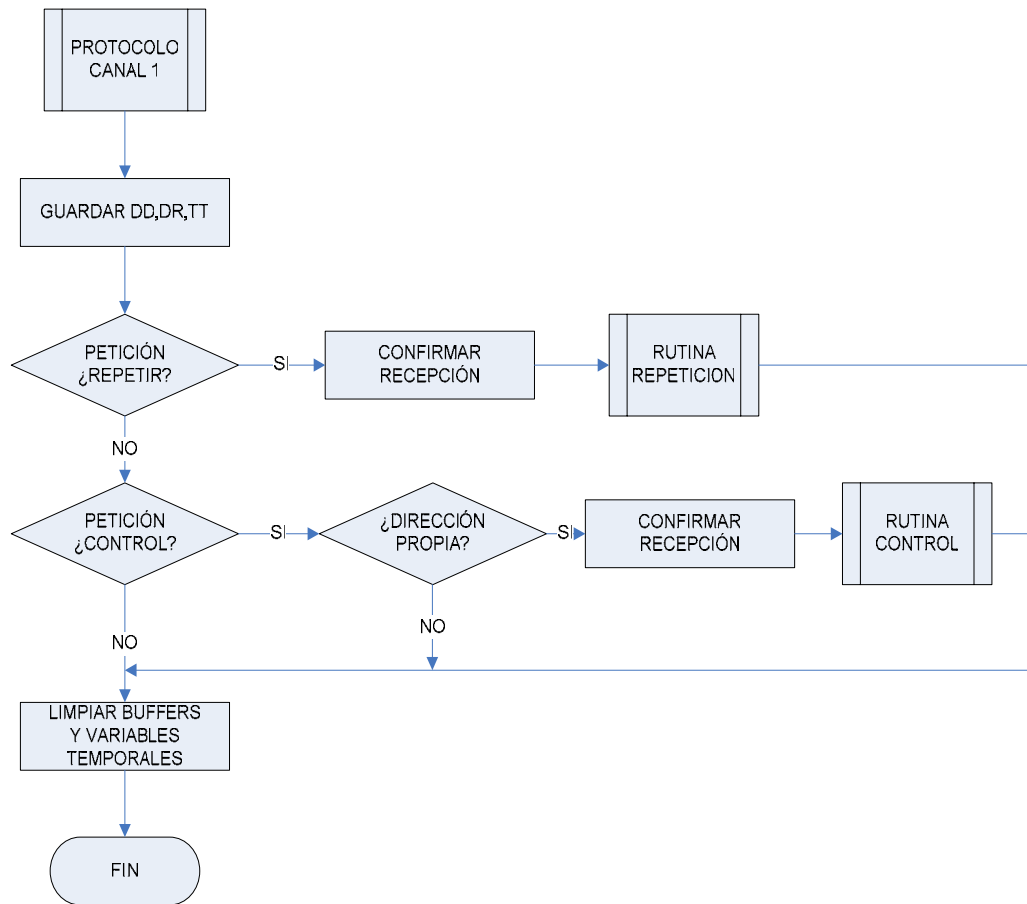


Figura 20. Diagrama de flujo de la rutina para manejo del mensajes entrantes en el canal de control

Por su parte, si ha llegado un mensaje por el canal de alarmas, se ejecuta la rutina “Protocolo Canal 2”. En esta rutina también se almacenan en variables temporales los campos que conforman la cabecera del paquete, a saber DD, DR y TT; los cuales servirán para configurar los mensajes salientes. Sólo podría recibirse un mensaje de alarma (TT=5), el cual se verifica que vaya dirigido al CCGR y luego se confirma la recepción de dicho mensaje al elemento que lo envió (cuya dirección es DR) y se pasa a la rutina de mensajes salientes en el canal de alarmas (en la cual se realizará el proceso de entrega hacia el CCGR) (ver figura 21).

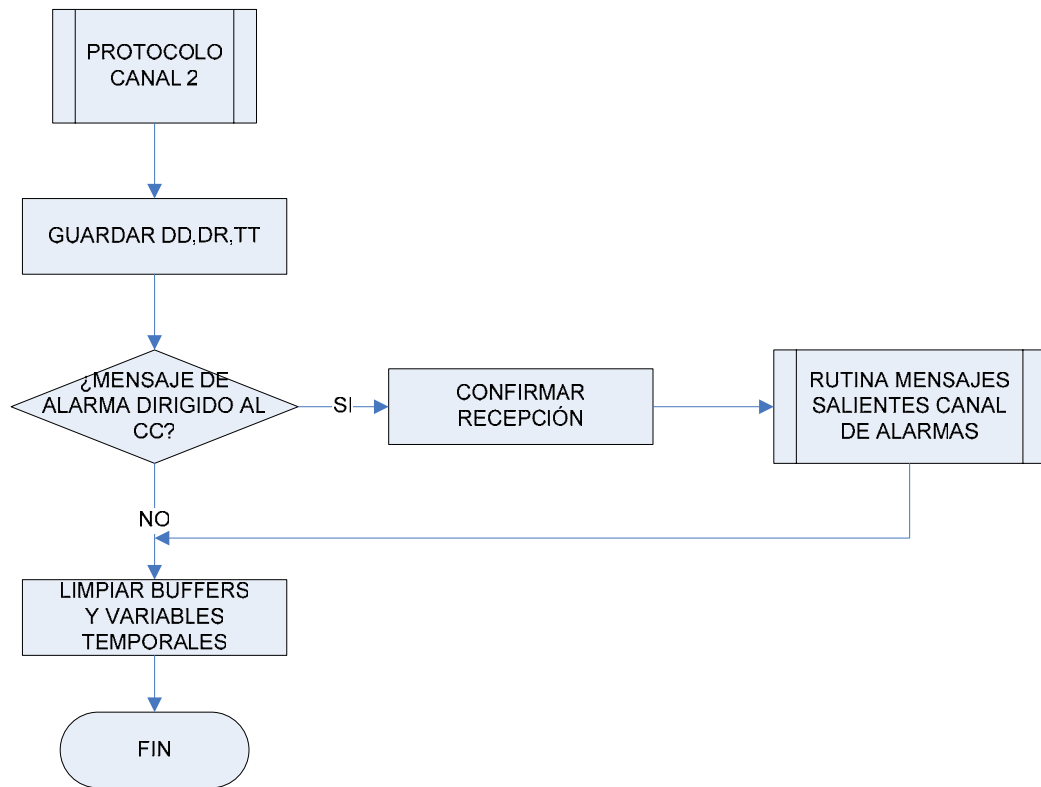


Figura 21. Diagrama de flujo de la rutina para manejo del mensajes entrantes en el canal de alarmas

El funcionamiento detallado del protocolo se describe en el Trabajo de Grado “Diseño e implantación de un protocolo de comunicaciones para un sistema de seguridad inalámbrico” presentado por el Br. Boris Roa.

7. Componentes del sistema en las redes de nivel inferior

Las redes de nivel inferior están conformadas por los dispositivos sensores y actuadores inalámbricos. Aunque puede manejar cierta cantidad de actuadores inalámbricos, el sistema está orientado principalmente a seguridad. Por tal razón, se ha hecho un esfuerzo especial en diseñar una variedad de dispositivos sensores. Los

sensores son módulos conformados por un sensor (de presencia, de vibración, de apertura o de humo) dotados con un sistema transmisor de datos digital en la banda de 400 MHz. Por su parte, los actuadores son módulos dotados de una salida de contacto seco a relé y un sistema receptor de datos digital en la banda de 400 MHz.

La estructura de una red de nivel inferior es de estrella centralizada (en un MZ). En dicha red se maneja un máximo de 64 sensores y 64 actuadores. La figura 22 muestra la estructura de una red de nivel inferior. La comunicación en esta red es unidireccional (los dispositivos sensores han sido dotados únicamente de transmisor y los actuadores únicamente de receptor) ya que esto reduce sensiblemente los costos del sistema. Por tal razón, no es posible desarrollar un protocolo de comunicaciones bidireccional en estos enlaces. El único terminal de la red de nivel superior que puede manejar estas subredes es el módulo MZ.

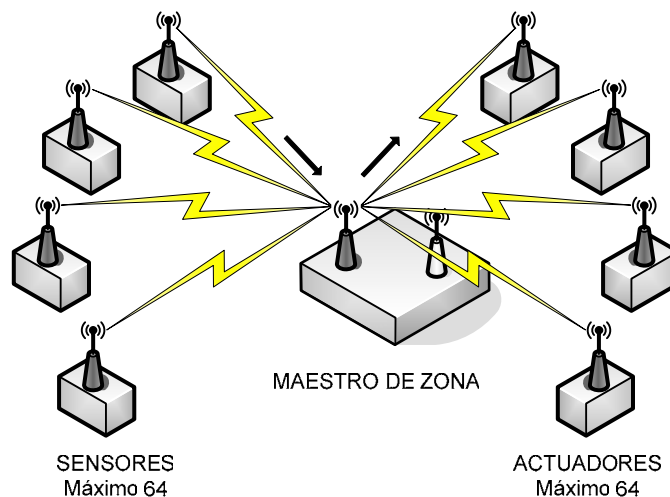


Figura 22. Estructura de las redes de nivel inferior

Los elementos de la red de nivel inferior no son configurables de forma remota, pero dado que sus parámetros son leídos de la memoria EEPROM interna, estos elementos pueden configurarse antes de entrar a funcionar dentro de la red.

8. Módulos de comunicación seleccionados para los elementos de la red de nivel inferior

Para las redes de nivel inferior se han seleccionado los transmisores TLPXXXA¹⁴ y los receptores RLPXXXA¹⁵ de Laipac Technology Inc. (ver figura 23). Sus características básicas son las siguientes:

- Modulación ASK
- Potencia de Salida 14 dBm @ 5 V (Transmisor)
- Velocidad máxima de transmisión de datos 4800 bps
- Sensibilidad -110 dBm (Receptor)

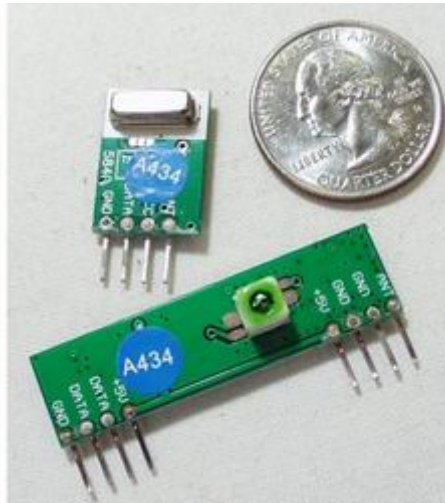


Figura 23. Módulos TLPXXXA y RLPXXXA de Laipac Technology Inc.

¹⁴ TLP434A, TLP315A y TLP418A

¹⁵ RLP434A, RLP315A y TLP418A

9. Modulación y codificación en los elementos de la red de nivel inferior

La técnica empleada para la modulación de los datos es ASK (Amplitude Shift Keying), sobre tres frecuencias portadoras: 433.92 MHz, 418 MHz y 315 MHz. La velocidad máxima de transmisión de datos en los módulos de la banda de 400 Mhz es de 4800 bps. Sin embargo, se decidió emplearlos a 2400 bps a fin de mejorar su desempeño.

Se empleó la codificación de datos según el código Manchester, un código de modulación bifásico en el cual un flanco de subida (transición de 0 a 1) representa un 1 lógico y un flanco de bajada representa un 0 lógico¹⁶. Esta codificación es una modulación en fase digital, lo cual facilita su implementación en sistemas digitales como el microcontrolador. Adicionalmente, facilita el sincronismo con el receptor y proporciona una mejor relación señal a ruido en comparación con otras técnicas como la modulación en frecuencia. La codificación Manchester ha sido probada y empleada ampliamente en diversos sistemas de comunicación como las redes Ethernet. Esta codificación se empleó debido que los módulos inalámbricos tienen rechazo hacia los niveles DC modulados. Sin embargo, la codificación Manchester reduce la velocidad de los datos a la mitad, por lo cual la velocidad real de transmisión de datos en el aire es de 1200 bps, velocidad aún suficiente para el bajo volumen de datos a transmitir.

La comunicación se efectúa cuando ocurre un evento (detección), y por reporte periódico.

¹⁶ Estándar IEEE 802.4

10. Estructura de datos en las redes de nivel inferior

Las tramas que se manejan en las redes de nivel inferior tienen la forma presentada en la figura 24.

Sincronismo de bits	Sincronismo de bytes	Dirección	Zona Asignada	Dato	CRC
---------------------	----------------------	-----------	---------------	------	-----

Figura 24. Estructura de datos en las redes de nivel inferior

En cada transmisión el sensor envía una trama conformada por 5 bytes. La tabla 3 muestra la descripción de cada uno de ellos.

Tabla 3. Descripción de los campos de la trama usada en las redes de nivel inferior

Byte	Descripción
1	Sincronismo de bits
2	Sincronismo de bytes
3	Dirección del sensor
4	Zona asignada (dirección del MZ correspondiente)
5	Dato a transmitir
6	CRC 8 bits

Para verificar la validez de los datos enviados al aire se utiliza como código de verificación de errores CRC de 8 bits, el cual se calcula sobre los bytes 3, 4 y 5.

11. Modo de comunicación en las redes de nivel inferior

Dado que no hay forma de verificar que la información llegó, se optó por realizar el envío sucesivo de tramas un número específico de veces, separadas entre sí por un tiempo pseudo-aleatorio constante para cada transmisión (ver figura 25).

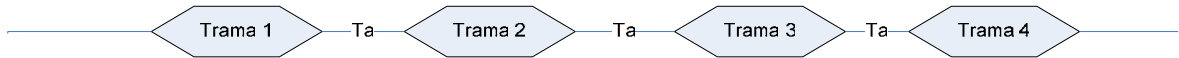


Figura 25. Modo de comunicación en las redes de nivel inferior (Ta= tiempo pseudo aleatorio)

Esta forma de acceder al medio reduce la probabilidad de colisión en el aire, permitiendo que el receptor capte alguna de las tramas. El número de veces que el dispositivo repite la trama es programable.

12. Redundancia en los elementos de la red

Todos los elementos de la red de nivel superior pueden tener respaldo. La redundancia se plantea como una red paralela configurada en modo respaldo, de modo que su comportamiento es inactivo con respecto a la transmisión de datos, pero activo en la recepción a fin de mantenerse actualizado con el elemento principal. Esto significa que el módulo principal tiene la misma dirección que su respaldo correspondiente, y la única diferencia entre ellos radica en cómo se halla configurado la entrada principal/respaldo y el registro de memoria principal/respaldo para su operación (ver tabla 4). Sólo bastará con escribir el registro correspondiente para invertir la operación de los dispositivos. Esto es aplicable tanto a los MZ como a los RP, ya que los CA no requieren tener respaldo.

La posibilidad de cambio de estado principal / respaldo no es automática, el CCGR de control lo hará en caso necesario¹⁷.

Tabla 4. Modos de configuración para respaldo

Entrada Principal / Respaldo	Registro (Hexadecimal)	Estado
Entrada activa	0000	Principal
Entrada inactiva	0000	Respaldo
Entrada activa	FFFF	Principal
Entrada inactiva	FFFF	Respaldo

13. Compatibilidad con elementos que operan en protocolo MODBUS

En el la redes de nivel inferior no se maneja el protocolo MODBUS, por tal razón un equipo que comparta la misma capa física no será compatible en absoluto. Si un elemento opera en protocolo MODBUS estándar y tiene la misma capa física de la red de nivel superior, requeriría de una pasarela que empaquetara el mensaje MODBUS en la misma capa de enlace manejada en el sistema para ser compatible en la red de nivel superior; ya que dicho nivel maneja las funciones 1, 2, 3, 4, 5, 6, 15 y 16 del estándar embebido en su propia capa de enlace. En este trabajo no se contempla el diseño de esta pasarela para compatibilidad con dispositivos MODBUS.

14. Sistema de pruebas

El modo de prueba es un algoritmo que permite a los módulos de la red de nivel superior determinar el porcentaje de enlace que poseen en el canal de control y en el canal de alarmas. Este algoritmo consiste en que un módulo del sistema es

¹⁷ En el presente trabajo, debido a que se construyó un número limitado de equipos, no fue posible montar equipos en modo respaldo.

configurado de forma remota por el CCGR para enviar un número de tramas a otro módulo en ambos canales y contabilizar cuantas transmisiones resultaron exitosas.

Para activar el modo de prueba, el CCGR escribe en el registro de pruebas de la memoria interna del módulo correspondiente la dirección de destino de las pruebas y el número de las mismas. Una vez concluido el proceso de escritura, el módulo comienza a realizarlas de inmediato. Una vez terminada las pruebas (el tiempo es proporcional al número de ellas) el módulo coloca 0 en este registro y escribe en el registro de resultado de pruebas de su memoria interna el resultado de las mismas, a fin de que el CCGR lo lea y determine el porcentaje de conexión en cada canal para ese módulo específico. De este modo, se puede probar la capacidad de enlace en los niveles de la red. Todos los elementos de la red de nivel superior poseen este algoritmo.

CAPÍTULO III

ESTRUCTURA Y CARACTERISTICAS DEL MÓDULO MAESTRO DE ZONA

1. El papel del Maestro de Zona en el sistema

El módulo Maestro de Zona (MZ), es el elemento del sistema encargado de recoger la información desde los sensores inalámbricos, y de procesar esa información para hacerla llegar hasta el módulo CCGR; así como recibir información desde el CCGR para activar o desactivar módulos actuadores inalámbricos. También puede recibir información desde el CCGR para operaciones de lectura / escritura de registros internos y operaciones de lectura de entradas locales y lectura / escritura de salidas locales. El MZ no tiene la capacidad de actuar como repetidor en la red de nivel superior.

Desde el punto de vista de la arquitectura del sistema, el MZ representa un elemento terminal de la red en árbol de ramales entrelazados de nivel superior y el nodo central de una de las redes (en estrella) de nivel inferior de un máximo de 64 sensores y 64 actuadores que operan en la banda de 400 MHz (ver figura 26).

El MZ incluye los algoritmos y sistemas necesarios para:

- Configuración, transmisión y recepción en dos canales en el módulo TRF-24G en la banda de 2.4 GHz.
- Transmisión y recepción para el módulo de transmisión en la banda de 400 MHz.

- Manejo del protocolo de enlace y red en el canal de control y en el canal de alarmas.
- Lectura del nivel de batería.
- Detección de conexión del transformador y reporte de alarma por desconexión.
- Revisión de estado de reporte de sensores asignados.
- Generación de alarmas de diversa índole provenientes de los sensores inalámbricos y generados por eventos locales.
- Manejo de información en memoria RAM y EEPROM interna.
- Cálculo de CRC para adjuntar a paquetes en el nivel superior de red.
- Envío de datos vía RS232 a 9600 baudios para monitoreo.

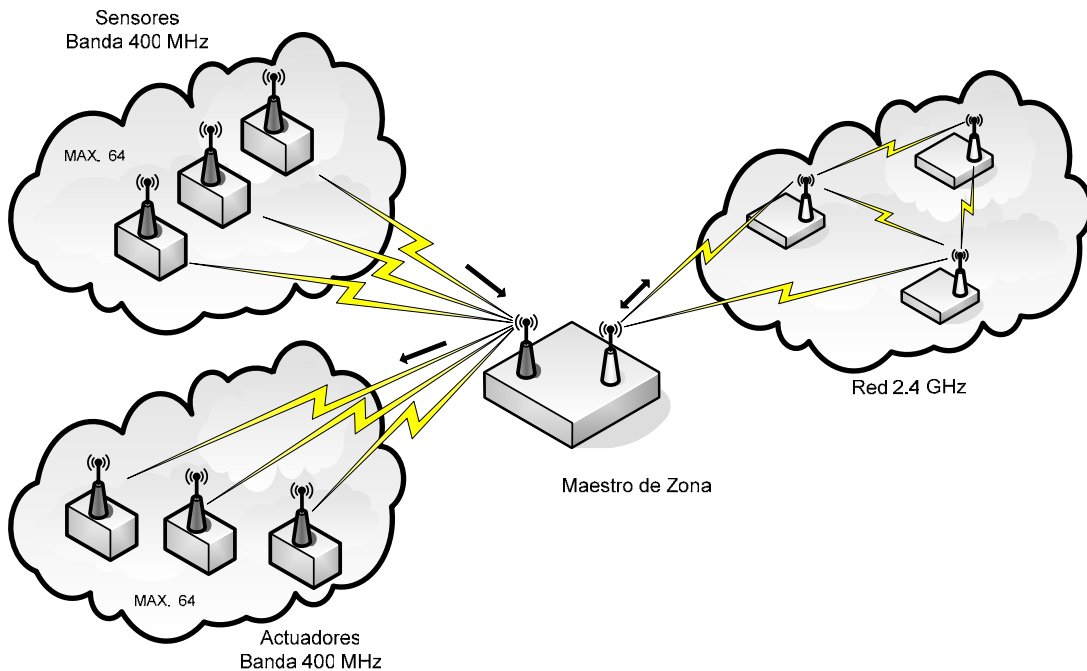


Figura 26. Posición del módulo MZ en la red

2. Estructura del Modulo Maestro de Zona

El módulo MZ está conformado por un microcontrolador central, un microcontrolador receptor que maneja un módulo de recepción RLPXXX en la banda de 400 MHz, un microcontrolador transmisor que maneja un módulo de transmisión TLPXXX en la banda de 400 MHz, un módulo transceptor para la banda de 2.4 GHz TRF-24G, 6 entradas a pull-up, una salida local a relé, un sistema de recarga de la batería y conversión A/D del nivel de carga, un sistema de conversión A/D para detección de conexión del transformador de alimentación desde la línea y un puerto de comunicación serial a 3.3V. El diagrama de bloques del MZ¹⁸ puede verse en la figura 27. Por su parte, la tabla 5 muestra las entradas del MZ y su uso.

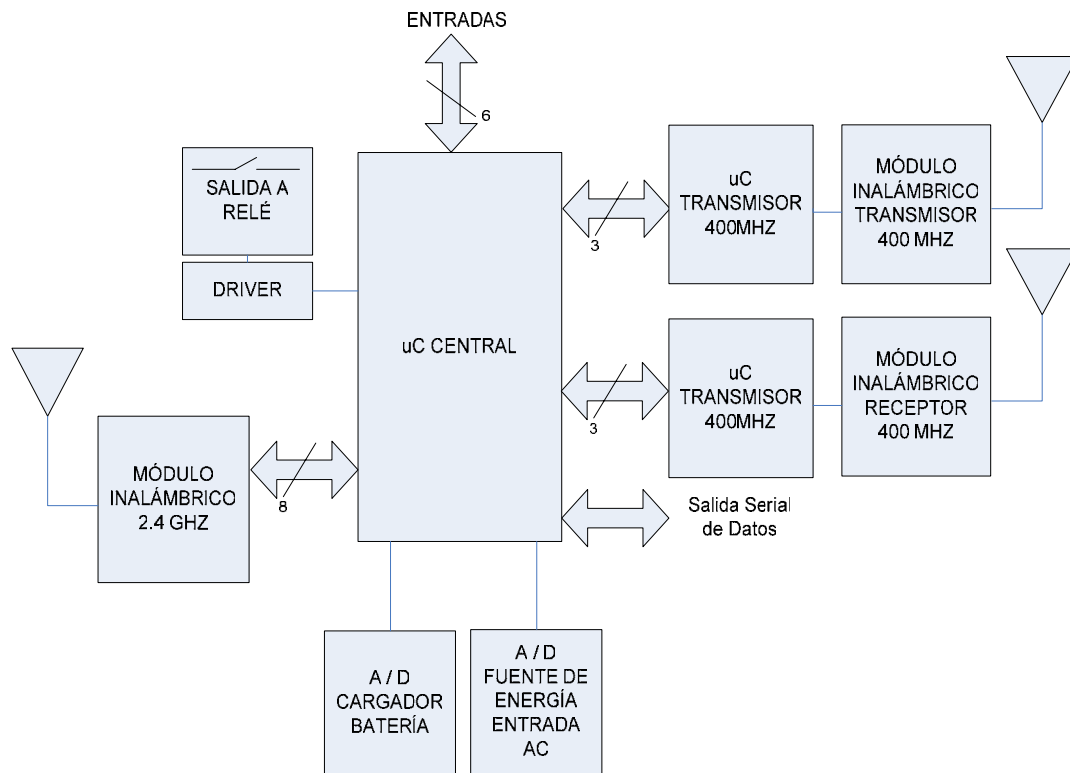


Figura 27. Diagrama de bloques del módulo MZ

¹⁸ Tanto el diagrama esquemático como el de circuito impreso pueden verse en el anexo 1.

Tabla 5. Entradas del MZ y usos asignados

Entrada	Identificador	Descripción
1	Auto reinicio	Al activarse, se reinicia el sistema, se toman los valores por defecto y se actualiza el valor de referencia de nivel de batería
2	Auxiliar	Uso no definido
3	Auxiliar	Uso no definido
4	Auxiliar	Uso no definido
5	Principal / Respaldo	Funciona según tabla 4 (presentada en el Capítulo I)
6	Detección de violación	Al activarse, se genera una alarma por violación

Se colocaron dos módulos independientes basados en microcontroladores dedicados para la transmisión y la recepción en la banda de 400 MHz. Debido a que en esta red de nivel inferior no se maneja un protocolo en el cual pueda verificarse la llegada de los datos, es de mucha importancia disponer de comunicación full duplex, en particular en el caso de la recepción que debe ser continua e ininterrumpida en virtud de que no debe perderse información. La pérdida de información en la recepción para la banda de 400 MHz implica perder el reporte de un evento y las consecuencias no favorables que ello acarrearía. Colocar de manera separada las tareas de transmisión y recepción en microcontroladores dedicados es una ventaja en este caso dada la estructura de diseño del sistema.

Estos microcontroladores dedicados tienen diversas funciones específicas. En el caso del procesador de recepción en 400 MHz, éste maneja el sincronismo de las comunicaciones en el aire, realiza la decodificación Manchester, verifica que los

datos que se reciben no tienen errores a través del cálculo y comparación del CRC de 8 bits y maneja una comunicación sincrónica con el microcontrolador central. Éste interrumpe al microcontrolador central ante la llegada de un paquete colocando un terminal en el nivel lógico correspondiente para proceder con la transferencia. Mientras el microcontrolador central no recoja la data del procesador de recepción, no se perderá el último mensaje a menos que llegue uno nuevo.

En el caso del procesador de transmisión en 400 MHz, éste tiene como función empaquetar los mensajes procedentes del microcontrolador central, calcular y adjuntar el CRC de 8 bits en los paquetes salientes y realizar la codificación Manchester. Cuando el microcontrolador central procede a enviar un paquete a través del microcontrolador transmisor, éste es interrumpido cuando un terminal del microcontrolador central se coloca en nivel lógico correspondiente, para proceder entonces con la transferencia del paquete saliente.

De modo que el procesador central del MZ no se ocupa con las tareas de empaquetamiento, sincronismo, codificación ni verificación de errores de los paquetes que transmite o recibe relacionados con la banda de 400 MHz.

Como ya se ha mencionado, el módulo MZ ha sido diseñado como el elemento terminal de la red de nivel superior. Por tal razón, es posible que en algunos casos se necesiten módulos repetidores para lograr la interconexión entre estos y el CCGR.

Los MZ sólo pueden operar en una de los tres canales disponibles (315,418 y 433.92 MHz) de la banda de referencia de 400 MHz, los cuales son utilizados para recibir datos desde los sensores o para transmitirlos a los actuadores (elementos de la red de nivel inferior). Para evitar colisión de datos entre paquetes entrantes y paquetes salientes, la transmisión y la recepción operan en canales diferentes para un mismo MZ.

Cada MZ puede manejar un máximo de 64 sensores inalámbricos y 64 actuadores inalámbricos. Se ha limitado el número de terminales en el nivel inferior para no congestionar el canal debido a colisiones y exceso de información en el aire.

El MZ, a través de una de sus entradas locales, ha sido programado para detectar violación del módulo a través de un pulsador pequeño presionado constantemente contra la superficie donde se realice la instalación o un detector de vibración. Adicionalmente, el MZ tiene una salida local a relé, para ser utilizada como alarma propia en caso de violación al módulo, o según se maneje desde el CCGR del sistema¹⁹. La programación de los MZ puede hacerse de forma remota desde el CCGR.

3. Distribución de los registros internos de operación del MZ

A fin de que el módulo funcione más rápidamente y más acorde con el protocolo que se maneja en la capa de red, el cual opera sobre registros de memoria de 16 bits, los espacios de memoria también son de 16 bits. Todas las posiciones de la memoria son de lectura / escritura. Por tal razón, es posible leer y escribir los registros internos de trabajo, y configurar el equipo de forma remota.

El MZ tiene 208 registros de memoria RAM para manejo de registros internos de operación distribuido en bloques de la siguiente manera (ver figura 28):

- 16 registros de valores de configuración (posiciones 0 a 15)
- 64 registros de manejo de dispositivos sensores (posiciones 16 a 79)
- 64 registros de manejo de dispositivos actuadores (posiciones 80 a 144)
- 64 registros de rutas de acceso (posiciones 144 a 208)

¹⁹ Para mayor información, véase el anexo 2, el cual contiene el diagrama de flujo del programa principal del MZ

00h~0Fh	Valores de Configuración
10h~4Fh	Manejo de Dispositivos Sensores
50h~8Fh	Manejo de Dispositivos Actuadores
90h~CFh	Rutas de Acceso

Figura 28. Mapa de memoria del módulo MZ

3.1- Registros de valores de configuración

En este espacio de memoria comprendido entre las posiciones 0 y 15 están ubicados los parámetros de funcionamiento propio del dispositivo MZ, a saber:

- Dirección del dispositivo. Representa el número de identificación del dispositivo, a la cual deben dirigir los paquetes otros elementos para lograr la comunicación con el dispositivo en cuestión. Esta dirección está comprendida entre 1 y 247. Es la misma para el canal de control y el canal de alarmas. Valor por defecto: 51.
- Canal de control (ChC). Es el canal de la banda de 2.4 GHz que el MZ usará para recibir y enviar mensajes de solicitud o configuración. Esta comprendido entre 0 y 124. El canal de control será $2400 \text{ MHz} + \text{ChC} * 1\text{MHz}$. El canal de alarmas será colocado automáticamente en $\text{ChC} + 8$, es decir $2400 \text{ MHz} + \text{ChC} * 1\text{MHz} + 8\text{MHz}$ ²⁰. Valor por defecto: 1.

²⁰ Esto se hace por limitaciones impuestas por el transceptor TRF-24G

- Registro de Principal / Respaldo. Este registro actúa en conjunto con la entrada principal / respaldo para definir el modo de operación del MZ según la tabla 4 del Capítulo I. Valor por defecto: 0.
- Registro de estado de la batería. Este registro contiene el porcentaje de carga de la batería. Valor por defecto: 0. (Este valor se actualiza 1 segundo después de encender el MZ)
- Tipo de Dispositivo. Contiene un número que permite identificar si el dispositivo es un MZ, un RP o un CA por parte del CCGR. En el caso de los módulos MZ el valor por defecto es 1, para CA es 2 y para RP es 3.
- Dirección del Centro de Control. Será el número de identificación del CCGR para el MZ. A esa dirección dirigirá todos los mensajes de alarma y de respuesta de querellas. Esta dirección está comprendida entre 1 y 247. Valor por defecto: 153.
- Multiplicador de base de tiempo de revisión de reporte de sensores asignados. El algoritmo de revisión de estado de reporte de sensores asignados opera según una base de tiempo de 1 segundo. Escribiendo en este registro de 16 bits, puede hacerse que el microcontrolador revise cuáles sensores no se reportaron dentro de ese tiempo y enviar un mensaje de alarma al CCGR. Este tiempo puede tener un máximo de aproximadamente 18 horas. Según la estructura de la red, los sensores inalámbricos deben estar programados para reportarse por lo menos 2 veces dentro de ese lapso para que el MZ no haga falsos reportes al CCGR. Valor por defecto: 21600 (6 horas).
- Multiplicador de tiempo de espera de respuestas en el protocolo de enlace. Será el tiempo que el dispositivo esperará antes de reenviar un mensaje, asumiendo que el dispositivo al cual lo envió no recibió el mensaje o no lo respondió por alguna razón. Base de tiempo 10 ms. Valor por defecto: 10.
- Número de repeticiones en la capa de enlace. En este registro se colocará el número de veces que el protocolo de enlace repetirá los mensajes si no se recibe confirmación. Valor por defecto: 10.

- Código especial de sensores: Byte alto: código de sensor violentado. Byte bajo: código de detección. Valor por defecto: 0102h.
- Código especial de sensores: Byte bajo: código de sensor reportado. Valor por defecto: 0003h.
- Monitoreo serial: Permite colocar el equipo sin monitoreo serial²¹ (0000h) o con monitoreo serial (FFFFh). (Valor por defecto: 0000h).
- Valor inicial A/D del nivel de batería. Valor por defecto: 0. (Este valor se actualiza 1 segundo después de encender el MZ²²)
- Registro de auto reinicio: Al colocar FFFFh, el equipo, se reiniciará y volverá al estado original con sus valores por defecto. Valor por defecto: 0.
- Registro de modo de pruebas: Byte alto: Dirección de destino de las pruebas. Byte Bajo: Número de pruebas a realizar en ambos canales. Cuando el CCGR escribe estos registros, el equipo comienza de inmediato al realizar las pruebas. Valor por defecto: 0.
- Registro de resultado de pruebas. Byte alto: Número de éxitos en el canal de control. Byte bajo: Número de éxitos en el canal de alarmas. Valor por defecto: 0.

La tabla 6 resume el uso de cada registro de memoria del bloque de registros de valores de configuración para el MZ.

²¹ A 9600 baudios

²² Después de aplicar un reinicio al sistema o al encenderlo por primera vez

Tabla 6. Registros de valores de configuración para el MZ

Dirección de Memoria (hexadecimal)	Contenido
0	Dirección del dispositivo
1	Canal de control
2	Principal / Respaldo
3	Porcentaje de la batería
4	Número de nivel o anillo
5	Dirección del centro de control
6	Multiplicador tiempo de revisión de sensores
7	Multiplicador tiempo de espera por respuesta
8	Número de repeticiones de la capa de enlace
9	Código de sensores: Violentado / Detección
10	Código de sensores: Normal
11	Monitoreo serial
12	Valor inicial A/D de batería
13	Registro de auto reinicio
14	Modo de pruebas
15	Resultado de pruebas

3.2 Registros de manejo de dispositivos sensores

Cada sensor asignado a un MZ es manejado como un registro interno de memoria. Hay 64 posiciones de memoria para los registros de sensores asignados al MZ (posiciones 16 a 79). En cada uno estos registros de memoria, de 16 bits, el

nibble superior indica si el dispositivo ha sido habilitado, el siguiente indica si se ha reportado, y en el byte inferior queda almacenado el último dato enviado por el sensor correspondiente (ver figura 29). Se reflejará el código del estado del sensor en la posición correspondiente de memoria interna del MZ.

Word

Nibble de Habilitación	Nibble de Reporte	Byte de Estado
---------------------------	----------------------	----------------

Figura 29. Estructura de los registros de memoria de manejo de sensores

Para evitar algoritmos de búsqueda que consumen más tiempo en el microcontrolador y requieren algoritmos más complejos, las posiciones de memoria corresponden a la dirección del sensor correspondiente más un índice. De este modo, el espacio para almacenar las direcciones adscritas al MZ es constante. La dirección de memoria 16 corresponde al sensor 1.

En el campo “Habilitación” se colocará Fh si el dispositivo está habilitado y 0h si está deshabilitado. Así, si el dispositivo MZ recibe un mensaje, busca por direccionamiento directo en la memoria y verifica rápidamente si está habilitado o no; para pasar a procesar el mensaje. Si el dispositivo recibe un mensaje proveniente de un sensor cuya dirección no esté habilitada en la tabla, este será notificado al CCGR como ‘dispositivo nuevo detectado’.

En caso de recibir un mensaje de reporte periódico, el microcontrolador coloca en el campo “Reporte” (inicialmente en 0h) el código correspondiente al estado “presente”, a saber Fh. Esta tabla, para el caso de elementos habilitados, deberá estar completamente llena en el lapso de revisión, tiempo en el cual el algoritmo de revisión de estado de reporte de sensores asignados verificará si uno o varios elementos no se reportaron para notificarlo hacia el CCGR. Una vez concluida

la verificación, los campos con la etiqueta “reporte” son colocadas nuevamente en 0h para comenzar de nuevo con el proceso de llenado. La revisión se realiza de acuerdo al período configurado en el registro de configuración de valores número 6.

Si desde uno de los sensores llega un mensaje que no es de reporte periódico, sino de alarma o violación de integridad, se verifica que el elemento esté habilitado en la tabla, y en caso afirmativo, se envía el mensaje directo al CCGR a través del canal de alarmas. De lo contrario, se seguirá reportando hacia el CCGR ‘nuevo dispositivo detectado’.

Para habilitar un dispositivo sensor en un MZ desde el CCGR, bastará con colocar F000h en el registro correspondiente del bloque de manejo de dispositivos sensores.

3.3 Registros de manejo de dispositivos actuadores

Se ha dispuesto de 64 posiciones de memoria para módulos actuadores (posiciones 80 a 144). Cada uno de estos registros está conformado por dos bytes: el byte superior indica al MZ que se desea realizar un cambio de estado de un actuador y el byte inferior indica al MZ el código a enviar al actuador correspondiente (ver figura 30).

Word



Figura 30. Estructura de los registros de memoria de manejo de actuadores

De forma similar a los registros de manejo de dispositivos sensores, en los registros de manejo de dispositivos actuadores las posiciones de memoria corresponden a la dirección del actuador correspondiente más un índice. De este modo, el espacio para almacenar las direcciones de actuadores adscritos al maestro de zona es constante. La dirección de memoria 80 corresponde al actuador 1.

Por ejemplo, para habilitar un cambio de estado para el actuador 15 instalado en la zona correspondiente al MZ en cuestión y enviarle por ejemplo, el código A7h; deberá colocarse en la posición de memoria 94 el código FFA7h. No hay limitaciones para el contenido del byte de código a enviar (mientras esté entre 0 y 255), lo cual permite hacer diversas aplicaciones para los actuadores. El actuador debe reconocer el código recibido y la acción a realizar.

3.4 Registros de rutas de acceso

Para el envío de paquetes, es posible que en algunos casos, el MZ no pueda acceder directamente hasta el CCGR sin pasar por un repetidor. Por tal razón, el MZ tiene una tabla de direccionamiento de mensajes salientes (posiciones 144 a 208), programable de forma remota, de 64 posibles rutas de salida (en orden de prioridad), con el siguiente formato mostrado en la figura 31.

Word

Byte de Dirección de Destino	Byte de Dirección de Envío
------------------------------	----------------------------

Figura 31. Estructura de los registros de memoria de rutas de acceso

Cada uno de estos registros está conformado por dos bytes: el byte superior representa la dirección de destino y el byte inferior indica al MZ la dirección de envío

del paquete. (Por ejemplo, un registro con el valor 582Ah indica que el MZ debe enviar el mensaje a la dirección 2Ah para llegar hasta el dispositivo 58h).

El orden en el cual están colocadas las direcciones de salida del mensaje determina la prioridad, ya que el MZ revisa las rutas empezando por la primera posición de la tabla de rutas y busca en orden creciente hasta encontrar el acceso o hasta recorrerla por completo.

Vale la pena mencionar que es irrelevante si los conjuntos de rutas para un mismo dispositivo se colocan en posiciones adyacentes o no, ya que el MZ buscará específicamente la dirección de interés e ignorará las demás. Si el CCGR está adyacente al MZ, se puede escribir en un registro cualquiera de rutas un Word cuya dirección de destino y dirección de envío sean iguales a la del CCGR.

El módulo MZ tiene programadas diversas acciones que se realizan de forma periódica. Una de ella es el refresco en memoria EEPROM interna de los bloques de registros de manejo de dispositivos sensores y actuadores, ya que el bloque de valores de configuración y el de rutas de acceso se almacenan en EEPROM después de cada cambio en RAM. La otra acción es la lectura del nivel de batería y la detección de presencia del transformador. La tabla 7 muestra los tiempos aproximados de realización de dichas acciones, los cuales no son reprogramables.

Tabla 7. Tiempos de realización de las acciones no reprogramables

Acción	Primera vez	Usualmente
Refresco de la memoria EEPROM	1 segundo	30 minutos
Lectura del nivel de batería y presencia de alimentación A/C	1 segundo	30 minutos

CAPÍTULO IV

ESTRUCTURA Y CARACTERÍSTICAS DEL MÓDULO REPETIDOR

1. El papel del Repetidor en el sistema

El módulo Repetidor (RP) es el elemento del sistema encargado de repetir y enrutar la información proveniente de otros dispositivos de la red de nivel superior del sistema (banda ISM 2.4 GHz). Este módulo se ha diseñado tomando en cuenta que debido a ciertas limitaciones de alcance, otros dispositivos no tienen la capacidad de acceder directamente al CCGR. Los elemento RP, dentro de la arquitectura del sistema, son los nodos en la red de árbol de ramales entrelazados (ver figura 32).

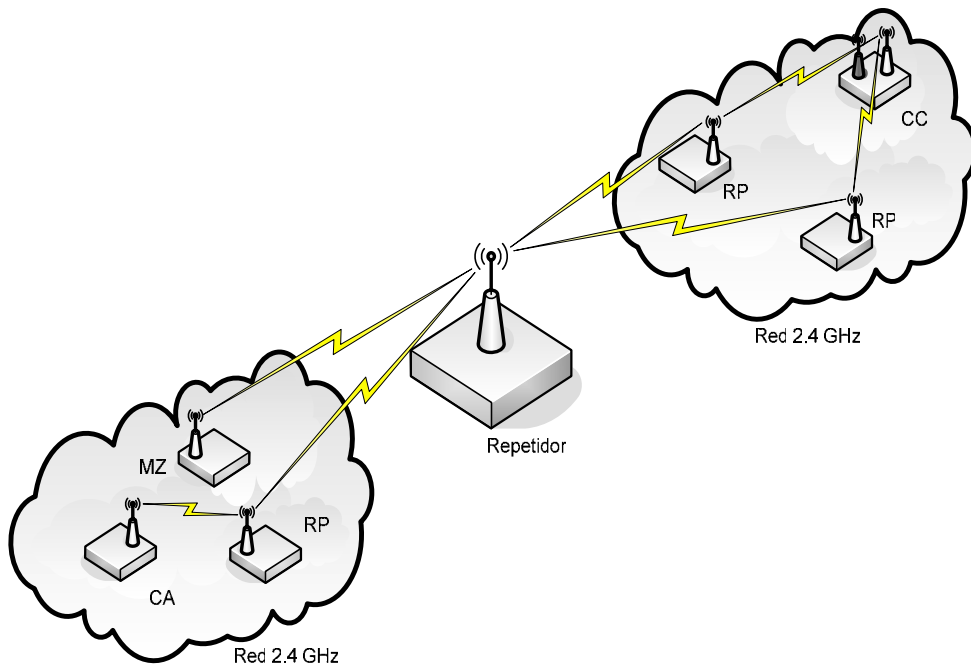


Figura 32. Posición del módulo RP en la red

Para el correcto funcionamiento del sistema, el CCGR tiene programados los repetidores inmediatos a los que tiene que enviar los paquetes para poder acceder a determinado terminal de la red del nivel superior (MZ ó CA). Asimismo, los MZ ó CA que accedan a la red para comunicarse con el CCGR deben tener almacenados los repetidores inmediatos a los cuales tiene que enviar los paquetes para lograr la comunicación. Esta información siempre está almacenada en el bloque de memoria de rutas de acceso, el cual está presente en todos los módulos.

Los repetidores más cercanos al CCGR son programados inicialmente, con lo cual, una vez puestos en funcionamiento, pueden dar acceso a otros módulos más lejanos y permitir su configuración sucesiva hasta llegar a los últimos elementos de la red. Esta configuración de la red se hace por niveles. Una vez puesta la red en funcionamiento, las rutas están completamente programadas y el CCGR envía paquetes directamente a los terminales; con lo cual la presencia y operación de los RP es irrelevante para él. Sólo se establece contacto directo con los RP cuando es necesario configurarlos o saber de su estado.

El RP incluye los algoritmos y sistemas necesarios para:

- Configuración, transmisión y recepción en dos canales en el módulo TRF-24G en la banda de 2.4 GHz.
- Manejo del protocolo de enlace y red en el canal de control y en el canal de alarmas.
- Lectura del nivel de batería.
- Detección de conexión del transformador y reporte de alarma por desconexión.
- Manejo de información en memoria RAM y EEPROM interna.
- Detección y reporte de violación al módulo.
- Cálculo de CRC para adjuntar a paquetes en el nivel superior de red.
- Envío de datos vía RS232 a 9600 baudios para monitoreo

2. Estructura del Modulo Repetidor

El módulo RP está conformado por un microcontrolador central, un módulo transceptor para la banda de 2.4 GHz TRF-24G, 3 entradas a pull-up, una salida local a relé, un sistema de recarga de la batería y conversión A/D del nivel de carga, un sistema de conversión A/D para detección de conexión del transformador de alimentación desde la línea y un puerto de comunicación serial a 3.3V²³ (ver figura 33).

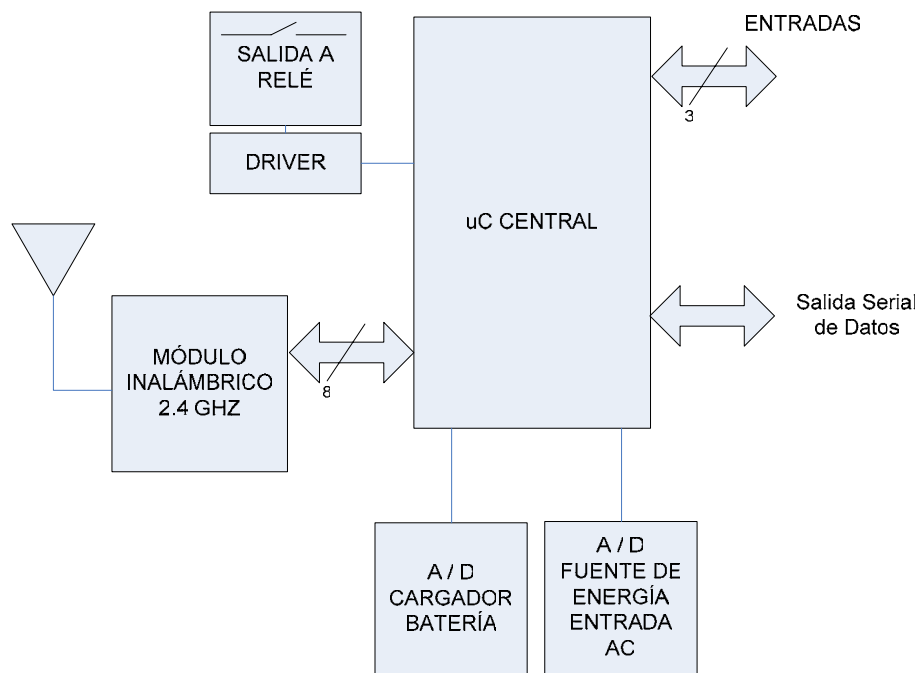


Figura 33. Diagrama de bloques del módulo RP

El RP, tal como el MZ, a través de una de sus entradas locales, ha sido programado para detectar violación del módulo a través de un pulsador pequeño

²³ Tanto el diagrama esquemático como el circuito impreso pueden verse en el anexo 3.

presionado constantemente contra la superficie donde se realice la instalación o de un detector de vibración. Adicionalmente, el RP tiene una salida local a relé (el cual pudiese ser activado desde el CCGR), para ser utilizada como alarma propia en caso necesario.

La programación de los RP puede hacerse de forma remota. En esa modalidad, el RP será visto como un terminal más de la red con dirección propia²⁴. La tabla 8 muestra las entradas del RP y su uso.

Tabla 8. Entradas del RP y usos asignados

Entrada	Identificador	Descripción
1	Auto reinicio	Al activarse, se reinicia el sistema, se toman los valores por defecto y se actualiza el valor de referencia de nivel de batería
2	Principal / Respaldo	Funciona según la tabla 4 (presentada en el Capítulo I)
3	Detección de violación	Si se activa, se genera una alarma por violación

3. Distribución de los registros internos de operación del RP

Tal como en el MZ, los espacios de memoria del RP también son de 16 bits. Todas las posiciones de la memoria son de lectura/escritura. Por tal razón, es posible leer y escribir los registros internos de trabajo y configurar el equipo de forma remota.

El RP tiene 144 registros de memoria RAM para manejo de registros internos de operación distribuido de la siguiente manera (ver figura 34):

²⁴ Para mayor información sobre el funcionamiento del módulo RP, véase el anexo 4, el cual contiene el diagrama de flujo del programa principal.

- 16 registros de valores de configuración (posiciones 0 a 15)
- 128 registros de rutas de acceso (posiciones 16 a 144)

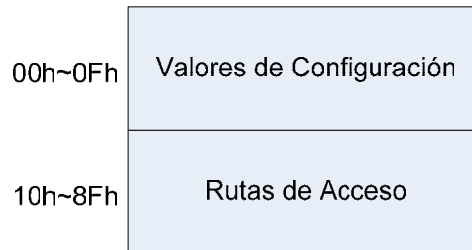


Figura 34. Mapa de memoria del módulo RP

3.1 Registros de valores de configuración

En este espacio de memoria comprendido entre las posiciones 0 y 15 están ubicados los parámetros de funcionamiento propio del dispositivo RP, de forma similar al dispositivo MZ, difiriendo por el hecho de que los registros 6, 9 y 10 no tienen un uso definido en este módulo. La tabla 9 resume el uso de cada registro del bloque de registros de valores de configuración.

Tabla 9. Registros de valores de configuración para el RP

Dirección de Memoria (hexadecimal)	Contenido
0	Dirección del dispositivo
1	Canal de control
2	Principal / Respaldo
3	Porcentaje de la batería
4	Número de nivel o anillo
5	Dirección del centro de control
6	Uso no definido
7	Multiplicador tiempo de espera por respuesta
8	Número de repeticiones de la capa de enlace
9	Uso no definido
10	Uso no definido
11	Monitoreo serial
12	Valor inicial A/D de batería
13	Registro de auto reinicio
14	Modo de pruebas
15	Resultado de pruebas

3.2 Registros de rutas de acceso

El módulo RP tiene un espacio de memoria dedicado al almacenamiento de las rutas que debe tomar la información que recibe para repetir a otros elementos de la red o para responder al CCGR (posiciones 16 a 144). El repetidor puede manejar un

máximo de 128 rutas (en orden de prioridad), incluyendo rutas alternas, programable de forma remota.

La estructura y el uso de los registros del bloque de registros de rutas de acceso del RP son idénticos a la del MZ. El RP utiliza estas rutas para dirigir mensajes salientes y direccionar mensajes a repetir. De igual modo, el tiempo de realización de las acciones no reprogramables es el mismo.

CAPÍTULO V

ESTRUCTURA Y CARACTERÍSTICAS DEL MÓDULO DE CONTROL DE ACCESO

1. El papel del Control de Acceso en el sistema

El módulo de Control de Acceso (CA), es el elemento del sistema encargado de gestionar la salida y entrada de los usuarios autorizados a determinado espacio controlado y reportar las alarmas asociadas a dicha gestión procesando la información para enviarla al CCGR. También puede recibir información desde el CCGR para operaciones de lectura / escritura de registros internos (incluso se puede ingresar nuevos usuarios en la memoria interna) y operaciones de lectura de entradas locales y lectura / escritura de salidas locales (por ejemplo, salidas y entradas utilizadas para control de acceso). El CA no tiene la capacidad de actuar como repetidor en la red de nivel superior. Desde el punto de vista de la arquitectura del sistema, el CA representa un elemento terminal de la red en árbol de ramales entrelazados de nivel superior (ver figura 35).

El CA incluye los algoritmos y sistemas necesarios para:

- Configuración, transmisión y recepción en dos canales en el módulo TRF-24G en la banda de 2.4 GHz.
- Manejo del protocolo de enlace y red en el canal de control y en el canal de alarmas.
- Lectura del nivel de batería.
- Detección de conexión del transformador y reporte de alarma por desconexión.
- Generación de alarmas por eventos locales.

- Manejo de información en memoria RAM y EEPROM interna y EEPROM externa vía I2C.
- Cálculo de CRC para adjuntar a paquetes en la red de nivel superior.
- Envío de datos vía RS232 a 9600 baudios para monitoreo.
- Transmisión y recepción de datos vía interfaz infrarroja.
- Manejo de una base de datos local de usuarios y control de entrada y salida.

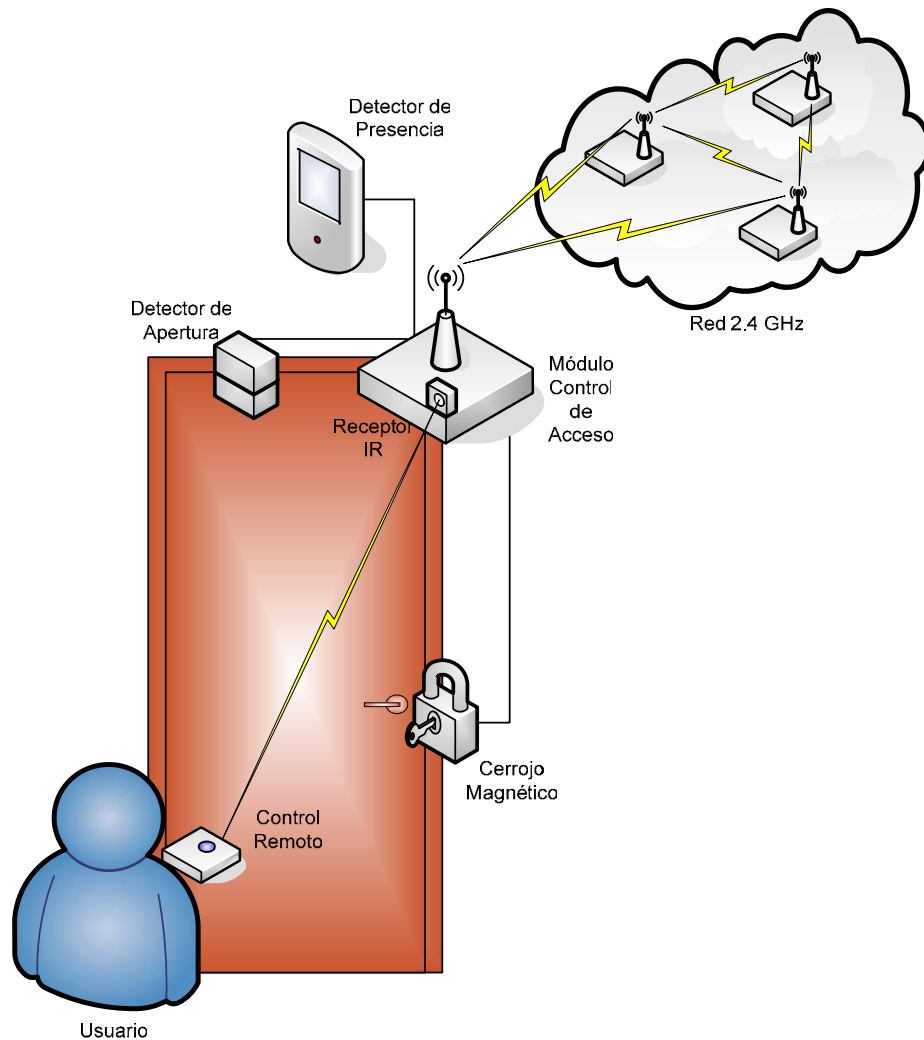


Figura 35. Estructura y posición en la red del módulo CA

2. Funcionamiento del módulo CA

El módulo CA está conformado por controles remotos infrarrojos de corto alcance los cuales poseen un teclado de tres pulsadores que permiten al usuario ingresar su propia clave para acceder al espacio controlado. La memoria de EEPROM externa del CA contiene la información asociada a todas las claves de usuario, información que puede ser actualizada a través del CCGR de forma periódica o cada vez que se presenten cambios.

El detector de apertura detecta si la puerta ha sido abierta (con o sin autorización del sistema, según sea el caso). El detector de presencia local verifica la presencia de usuarios dentro del espacio controlado. Por su parte, el cerrojo magnético libera el pasador de la puerta activando una de sus salidas locales a relé para que el usuario autorizado acceda al espacio al ingresar su clave usando el control remoto. El microcontrolador central del CA controla todos estos periféricos y es capaz de generar alarmas locales de forma autónoma.

El diagrama de flujo del CA es casi igual al del RP, sólo que éste no acepta la función de repetición e incluye una verificación de mensajes entrantes vía interfaz infrarroja.

Las condiciones de funcionamiento del sistema son las siguientes:

- El usuario debe usar su control remoto al momento de entrar y al momento de salir del espacio controlado.
- La clave de acceso está compuesta por una secuencia de 8 dígitos a marcar y se tienen 3 oportunidades de marcación programada, lo cual hace que la

probabilidad de acceso de un intruso que posea el control remoto de forma no autorizada sea muy baja²⁵.

- Cuando las oportunidades de marcación se terminan, el sistema no realiza la activación del cerrojo magnético y genera una alarma disuasiva y un informe dirigido al CCGR. Adicionalmente, el control remoto se bloquea durante un tiempo programado.
- Cuando la puerta es violada (evento que sería detectado por el interruptor magnético colocado en la junta de la puerta), el sistema generará una alarma disuasiva y un informe dirigido al CCGR.
- Cuando todos los usuarios han salido del espacio controlado, el módulo CA atiende la señal del detector de presencia local. Si se supone que no hay usuarios dentro del espacio controlado y el detector se activa, el sistema generará una alarma disuasiva y un informe dirigido al CCGR.
- El usuario posee una clave distinta a su clave usual de acceso denominada clave de pánico. Esta clave debe usarla el usuario cuando se encuentre sometido por un intruso para acceder al espacio. Esta clave permite el acceso aparentemente normal al espacio pero genera un informe pertinente al sistema maestro.

3. Estructura del módulo CA

El modulo CA está conformado por un microcontrolador central, un módulo transceptor para la banda de 2.4 GHz (TRF-24G), 6 entradas a pull-up, dos salidas locales a relé, un sistema de recarga de la batería y conversión A/D del nivel de carga, un sistema receptor infrarrojo doble, un sistema de conversión A/D para detección de conexión del transformador de alimentación desde la línea y un puerto de comunicación serial a 3.3V. El diagrama de bloques del CA se muestra en la figura 36²⁶. La tabla 10 muestra las entradas del CA y su uso.

²⁵ Véase el apartado **Control Remoto**, donde se dan más detalles al respecto.

²⁶ Tanto el diagrama esquemático como el circuito impreso pueden verse en el anexo 5

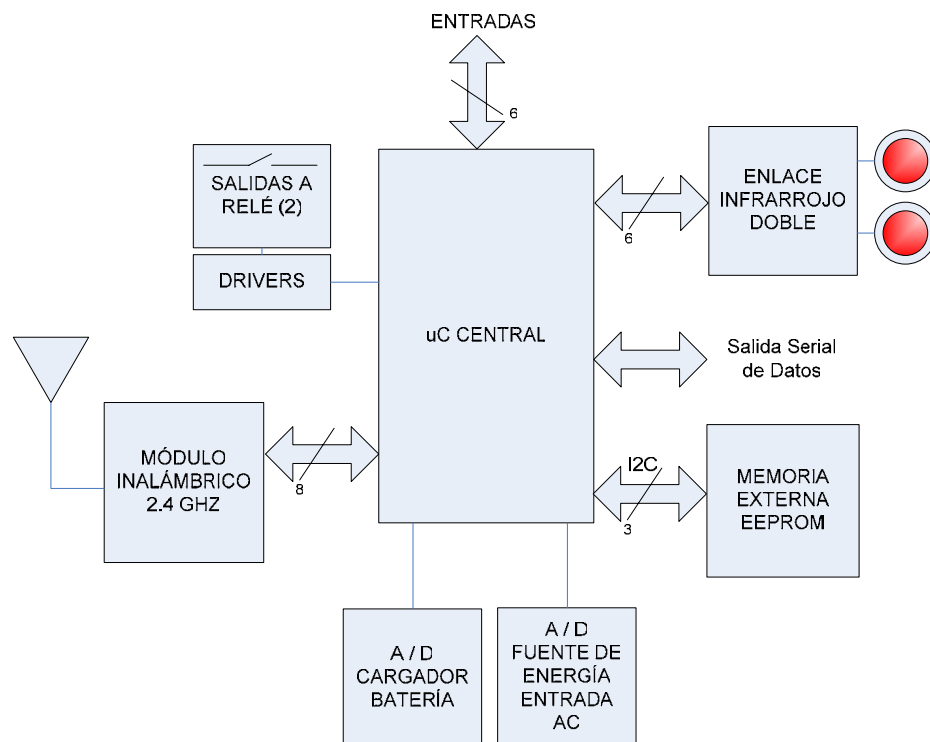


Figura 36. Diagrama de bloques del módulo CA

Tabla 10. Entradas del CA y usos asignados

Entrada	Identificador	Descripción
1	Auto reinicio	Al activarse, se reinicia el sistema, se toman los valores por defecto y se actualiza el valor de referencia de nivel de batería
2	Apertura	Se coloca un interruptor magnético con salida normalmente abierta para detectar la apertura de la puerta del espacio a controlar
3	Presencia	Se coloca un detector de presencia con salida normalmente abierta para monitorear la zona de acceso
4	Auxiliar	Uso no definido
5	Principal / Respaldo	Funciona según tabla 4 (presentada en el Capítulo I)
6	Detección de violación	Si se activa, se genera una alarma por violación

4. Distribución de los registros internos de operación del CA

Tal como en el MZ, los espacios de memoria del CA también son de 16 bits. Todas las posiciones de la memoria son de lectura/escritura. Por tal razón, también es posible leer y escribir los registros internos de trabajo y configurar el equipo de forma remota.

El CA tiene 88 registros de memoria RAM para manejo de registros internos de operación distribuido de la siguiente manera (ver figura 37):

- 16 registros de valores de configuración (posiciones 0 a 15)
- 8 registros para gestión de usuarios (posiciones 16 a 23)
- 64 registros de rutas de acceso (posiciones 24 a 87)

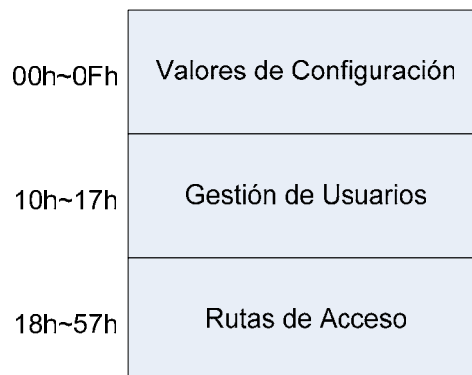


Figura 37. Mapa de memoria del módulo CA

4.1 Registros de valores de configuración

En este espacio de memoria comprendido entre las posiciones 0 y 15 están ubicados los parámetros de funcionamiento propio del dispositivo CA, de forma idéntica al dispositivo RP (Ver tabla 9 del Capítulo IV).

4.2 Registros de gestión de usuarios

En este espacio de memoria comprendido entre las posiciones 16 y 23 están ubicados 8 campos que permiten manejar indirectamente la memoria EEPROM externa donde se almacena tanto la clave de todos los usuarios como su estado (dentro o fuera del espacio controlado). Usando este bloque de memoria puede leerse tanto la clave como el estado de un usuario determinado, así como eliminar algún usuario o simplemente cambiar su clave de acceso. Se ha limitado en número de usuarios a un máximo de 2.000 por espacio controlado. La tabla 11 muestra uso de cada registro del bloque de registros de gestión de usuarios.

Tabla 11. Bloque de registros de gestión de usuarios

Dirección de Memoria	Contenido
16	Código de Escuela
17	Código de Facultad
18	Leer / Escribir
19	Número de Usuario
20	Clave de Usuario
21	Estado del Usuario
22	Estado de la Operación
23	Número de usuarios dentro del espacio

Los registros de gestión de usuarios tienen el siguiente uso:

- Código de Escuela: En este registro el CCGR debe escribir un código único y secreto de 16 bits, el cual será verificado para realizar cualquier operación de lectura o escritura en la memoria de almacenamiento de datos de usuarios. Valor por defecto: 0.

- **Código de Facultad:** De igual modo que en el caso anterior, en este registro también debe escribirse un código único y secreto de 16 bits, el cual será verificado al momento de leer o escribir. Valor por defecto: 0.
- **Leer / Escribir:** Este registro indica al sistema si el proceso es de lectura o de escritura (FFFFh indica escritura, 0000h indica lectura). Valor por defecto: 0000h.
- **Número de Usuario:** Cuando se realiza alguna lectura o escritura de los datos de usuario debe escribirse en esta posición de memoria el número de usuario, el cual debe ser inferior a la capacidad máxima de almacenamiento de usuarios (2.000). Valor por defecto: 0.
- **Clave de Usuario:** Si se está escribiendo una clave de usuario, debe colocarse en esta posición la nueva clave a escribir. Colocar 0 en este campo durante el proceso de escritura implica que se está borrando un usuario. Por otra parte, si se está realizando un proceso de lectura, este campo reflejará la clave del usuario que se esté leyendo. Valor por defecto: 0.
- **Estado de la Operación:** Este campo puede tomar diversos valores dependiendo del estado del proceso, a fin de que el CCGR realice las operaciones en el momento adecuado. Los valores que puede tomar este campo son los siguientes:

0	En espera
1	Código de Escuela o Facultad Inválido
2	Número de usuario sobrepasa la capacidad
3	Proceso de escritura completo
4	Proceso de lectura completo
5	Operación inválida

Valor por defecto: 0.

- **Estado del Usuario:** Al completarse el proceso de lectura de un usuario, este campo indica si el usuario está dentro del recinto controlado o afuera. (FFFFh indica adentro, 0000h indica afuera). Valor por defecto: 0.

- Número de usuarios en el espacio: Lleva la cuenta del número de personas que ocupan el espacio controlado. Valor por defecto: 0.

Para realizar cualquier operación relacionada con la gestión de usuarios, el CCGR debe leer el registro ‘Estado de la Operación’. Si dicho registro indica que el sistema está en espera, el CCGR puede realizar operaciones de lectura o escritura inmediatamente. Tanto el proceso de lectura como el de escritura de usuarios en el sistema pueden realizarse en dos operaciones. Para entender mejor el proceso, obsérvense los ejemplos que se plantean el anexo 6.

4.3 Registros de Manejo de Rutas de Acceso

El módulo CA tiene un espacio de memoria dedicado al almacenamiento de las rutas que debe tomar la información que recibe para repetir a otros elementos de la red o para responder al CCGR (posiciones 24 a la 87). El repetidor puede manejar un máximo de 64 rutas (en orden de prioridad), incluyendo rutas alternas, programable de forma remota. Estos registros tienen el mismo formato y condiciones de funcionamiento que en el módulo MZ.

5. Control Remoto

Para acceder al espacio controlado por el CA se plantea el uso por usuario de un teclado portátil de 3 dígitos con enlace infrarrojo. Para ello ha de colocarse en el mismo una clave de 8 dígitos. Al colocar el último dígito, el teclado emite a través de un led infrarrojo una trama de datos que contiene un código de 16 bits de código de usuario y 8 bits de verificación de errores. El usuario tiene hasta 3 oportunidades para acceder con su código, lo cual le da una probabilidad de acertar de 0.046%. Dado que se permite el acceso de 2000 usuarios en el espacio controlado, un intruso con el teclado tiene probabilidad de acertar el código de 0,0014 %, y puede identificarse a

través de la base de datos del administrador del sistema a quién le fue sustraído el teclado.

Una vez presionada la primera tecla, el usuario tiene unos 2 segundos aproximadamente para presionar la siguiente y así sucesivamente, hasta que termine de ingresar la secuencia. Cada vez que se presione una tecla, el tiempo se reinicia. Si transcurren los dos 2 segundos antes de presionar la tecla siguiente, el control vuelve a su estado inicial de espera de marcación. Mientras el tiempo de marcación está activo, un led luminoso permanece activo en el control remoto. El control remoto está basado en un microcontrolador. El diagrama de bloques se muestra en la Figura 38.

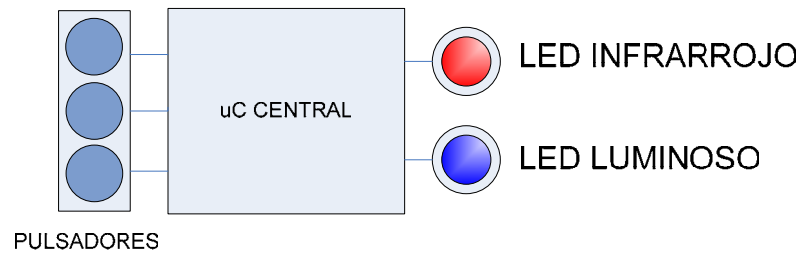


Figura 38. Diagrama de bloques del control remoto

Como ya se ha mencionado, el control remoto sólo permite 3 intentos para acceder al espacio controlado. Si en los tres intentos el usuario no consigue acceder, el control remoto envía una clave de intruso para que el módulo CA genere un informe hacia el CCGR y además la transmisión infrarroja del control remoto queda inhabilitada por unos cinco (5) minutos aproximadamente.

CAPÍTULO VI

ESTRUCTURA Y CARACTERÍSTICAS DE LOS SENSORES Y ACTUADORES DEL SISTEMA

Entre los sensores y actuadores diseñados para el sistema de seguridad prototipo se tienen:

- Sensor de incendio
- Sensor de apertura
- Sensor de vibración
- Sensor de presencia
- Actuador de contacto seco

1.- Módulos Sensores

Todos estos módulos están conformados por un transmisor TLPXXX de Laipac Technology Inc. en la banda de 400 MHz, un microcontrolador programado para transmitir los eventos, una entrada para adquirir el estado del sensor y otra entrada para autoprotección. En la figura 39 se puede apreciar el diagrama de bloques de un módulo sensor²⁷.

²⁷ Tanto el diagrama esquemático como el circuito impreso pueden verse en el anexo 7

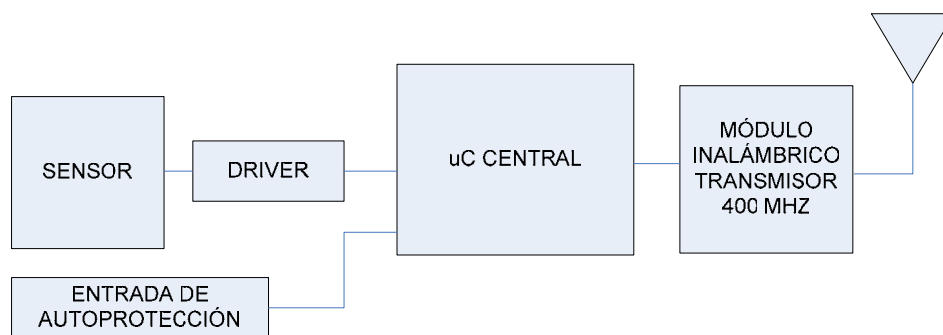


Figura 39. Diagrama del bloques de un módulo sensor

Como ya se ha mencionado, todos los módulos sensores y actuadores conforman redes de nivel inferior con arquitectura de estrella centralizada en un módulo MZ, el cual concentra los datos enviados por los sensores en la banda de 400 MHz y empaqueta esos eventos como alarmas para enviarlos hacia el CCGR en la banda de 2.4 GHz. En la figura 40 puede observarse la posición de los módulos sensores en el sistema.

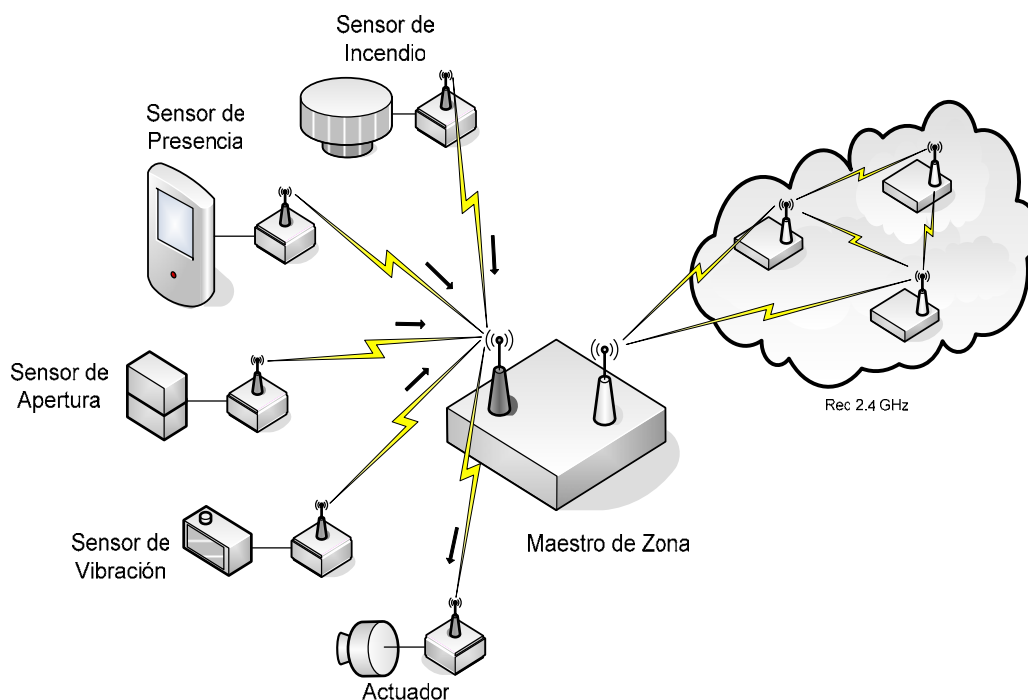


Figura 40. Posición de los módulos sensores en el sistema

Al encender un módulo sensor, el microcontrolador carga los valores de trabajo desde la memoria EEPROM interna. Esto permite que pueda configurarse cada sensor antes de entrar en operación programando los valores sobre dicha memoria sin necesidad de editar el programa. Los valores que el dispositivo lee desde la memoria EEPROM interna son los que se muestran en la Tabla 12.

Tabla 12. Valores de trabajo a cargar en la memoria EEPROM interna del sensor

Posición de Memoria (Hexadecimal)	Valor a Cargar
01	Dirección de sensor
02	Zona Asignada
03	Número de veces a repetir la trama
04	Código de reporte periódico
05	Código de detección
06	Código de violación de módulo
07	Multiplicador Tiempo de reporte 1 ²⁸
08	Multiplicador Tiempo de reporte 2

1.1. Módulo de detección de apertura

Es un módulo sensor dotado con un detector de apertura, el cual es un dispositivo magnético que cierra un contacto seco al activarse. Se suele utilizar en la junta de las puertas o ventanas para detectar apertura. Este tipo de sensores están clasificados entre los detectores de intrusión perimetrales. Este módulo puede ser empleado para detectar apertura en puertas, ventanas, o incluso muebles.

²⁸ Base de tiempo de 1 minuto

1.2. Módulo de detección incendio

Para el desarrollo este módulo se seleccionó un detector iónico de incendio, con batería de 9V y alarma sonora de 80 dB incorporada, por ser un detector muy fácil de instalar.

El uso de un detector iónico es ventajoso ya que son aptos para toda la gama de humos detectables y estables ante variaciones de presión, temperatura y corrientes de aire y permiten una detección precoz. Sin embargo, pueden dar falsas alarmas en ambientes con aerosoles, polvo, aire en movimiento, humedad elevada, concentración de humo de cigarrillos. Estos sensores pueden utilizarse para detectar desde fuegos latentes (pirolisis, fuegos de combustión lenta) hasta fuegos abiertos de llama viva y combustiones de sólidos y líquidos con humos visibles e invisibles (caso de llamas vivas).

En el ambiente comercial y educativo este sensor es uno de los más usados. Lo recomendable es tener un detector por cada 40 metros cuadrados. Los detectores de incendio descritos deben instalarse en el techo de la estancia, centrado con respecto a la estancia y a una distancia mínima de 50 centímetros de la pared. En general, los fabricantes recomiendan cambiarlos cada 10 años.

Este módulo se ha diseñado para detectar la señal que se envía a alarma sonora local del mismo sensor, la cual se activa inmediatamente ante una detección. El sensor iónico, el módulo sensor y la alarma, se alimentan de una batería de 9 VDC, la cual, debido a la muy poca frecuencia de activación garantiza gran duración. Para alimentar el microprocesador, se colocó un regulador de tensión a 5V.

1.3. Módulo de detección de vibración

Es un módulo sensor dotado con un detector de vibración, el cual se basa en una laminita mecánica que cierra un contacto seco al vibrar. Se suele colocar en los cristales de las ventanas para detectar ruptura del cristal. Este tipo de sensores se clasifican entre los detectores de intrusión perimetrales. Este sensor podría usarse para detectar golpes o ruptura en cristales o en objetos que no deben tocarse.

1.4. Módulo de detección de presencia

Es un módulo sensor dotado con un detector de presencia, el cual se clasifica como un detector volumétrico. Este tipo de detector, debe colocarse en una esquina de la estancia y en su parte superior, asegurando una orientación que logre la máxima cobertura posible y siempre alejado de cualquier fuente de calor, para evitar falsas alarmas.

En detectores volumétricos se suelen utilizar dos tipos de tecnologías distintas: infrarrojos y microondas. A través de la primera es posible detectar movimientos en el interior de la estancia como consecuencia de cambios de temperatura en el ambiente (por ejemplo, por el paso de una persona). El único inconveniente de este tipo de tecnología es el alcance, limitado a la estancia donde se encuentran o con visión directa. Por su parte, los detectores volumétricos con tecnología microondas disponen de un mayor alcance al traspasar paredes entre estancias. Sin embargo, su uso no resulta adecuado en viviendas (especialmente en edificios de viviendas) dado que movimientos en viviendas contiguas pueden afectar a la detección.

2. Actuador de contacto seco

Los actuadores están conformados por un receptor RLPXXX de Laipac Technology Inc. en la banda de 400 MHz, un microcontrolador que contiene el algoritmo de recepción y ejecución de las acciones y una salida a relé (corriente máxima 1A @ 110V). La figura 41 muestra el diagrama de bloques de un módulo actuador²⁹. Este actuador puede utilizarse para el control de cargas de forma remota, y también para la activación de mecanismos de alarma remotos.

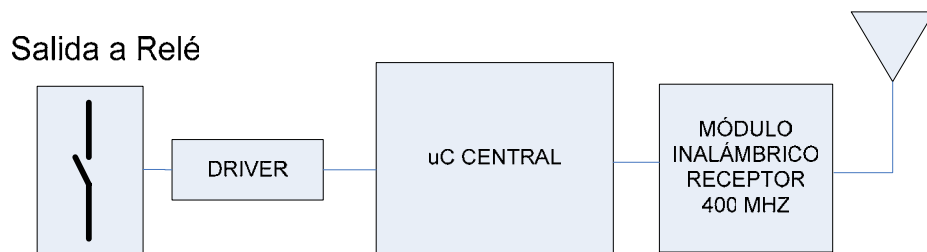


Figura 41. Diagrama del bloques de un módulo actuador

Tabla 13. Valores de trabajo a cargar en la memoria EEPROM interna del actuador

Posición de memoria (Hexadecimal)	Valor a Cargar
01	Dirección de actuador
02	Zona asignada
03	Código encendido
04	Código apagado

²⁹ Tanto el diagrama esquemático como el circuito impreso pueden verse en el anexo 8.

CAPITULO VII

PRUEBAS Y VALIDACIÓN DEL SISTEMA

Efectivamente, tal como se planteó en un principio, los requerimientos y las variables del sistema de seguridad se definieron completamente, empleando como base del estudio la investigación del estado del arte de los sistemas de seguridad comerciales y las características a las cuales los fabricantes prestan especial atención a la hora de ofrecer sus productos. Partiendo de dicha investigación, se definieron aspectos importantes para el presente proyecto. Uno de esos aspectos fue la arquitectura de la red, la cual debía soportar el montaje de todos los elementos vía interfaz inalámbrica en una edificación del tipo comercial o educativo; con lo cual se llega a la concepción de la arquitectura de red con estructura de árbol de ramales entrelazados. Una vez que la arquitectura de la red estuvo perfectamente definida, se seleccionaron los módulos adecuados para la transmisión de datos en el sistema (en términos de costos y prestaciones) para pasar a integrarlos en cada uno de los equipos que prestan servicios específicos dentro de la red.

Este proceso de diseño e integración de tecnologías generó el trabajo de definir el hardware y la programación del software de los elementos del sistema con lo cual se definen las tareas y el papel de cada equipo en la red.

Gracias a las ventajas que aporta por sí sólo el modulo de comunicaciones en la red de nivel superior y el algoritmo de codificación aplicado a los datos en todos los elementos de la red, se obtiene un nivel de transmisión segura de datos aceptable.

Vale la pena resaltar, que aunque en un principio se había propuesto el diseño de una interfaz desde una PC hacia la red para realizar la tarea de centro de control, es decir manejo de toda la red, se resolvió diseñar un módulo electrónico central, ya que el PC no ofrece la robustez que requiere la ejecución ininterrumpida de un programa. Todo este concepto generó el trabajo de diseño de lo que se denominó Centro de Control y Gestión de Red (CCGR), un módulo autónomo externo al PC conformado por una Unidad de Control (hardware dedicado a la gestión del sistema) y una Interfaz de Usuario (software que permite configurar la Unidad de Control y permite monitorear los eventos generados en la red), lo cual requirió la apertura de un Trabajo de Grado adicional³⁰. En el trabajo relacionado con CCGR se define el número de eventos que puede almacenar el sistema, ya que eso depende de la capacidad de almacenamiento del mismo.

De cualquier modo, podría decirse que el sistema obtenido en el presente trabajo supera en algunos aspectos a los sistemas de seguridad comerciales. Uno de esos aspectos es que es un sistema completamente inalámbrico para aplicaciones no residenciales. Adicionalmente, la capacidad de almacenamiento de eventos, el número de usuarios y zonas que se pueden manejar es superior al promedio. Adicionalmente provee facilidades para configuración y monitoreo.

A fin de verificar todos los aspectos relacionados con el diseño del sistema de seguridad, así como detectar cualquier posible falla y realizar las correcciones pertinentes, se hizo el montaje de una red prototipo de cuatro niveles conformada por los siguientes elementos:

- Red de nivel superior
 - o 2 Módulos MZ
 - o 3 Módulos RP

³⁰ “Sistema de Control Maestro para el Sistema de Seguridad Inalámbrico de la EIE de la UCV”, presentado por el Br. José Carrasquel.

- o 1 Módulo CA
- Redes de nivel inferior
 - o Red 1:
 - 2 Sensores de apertura
 - 2 Sensores de ruptura
 - 1 Sensor de incendio
 - 1 Sensor de presencia
 - 1 Actuador de uso general
 - o Red 2:
 - 2 Sensores de apertura
 - 2 Sensores de ruptura
 - 1 Actuador de uso general

Con los elementos mencionados anteriormente, se procedió a construir la red que se muestra en la figura 42. Efectivamente se realizó la configuración del equipo por niveles.

El prototipo se verificó realizando pruebas de comunicaciones para comprobar el efectivo funcionamiento del protocolo de enlace y red, en donde los paquetes realizaron cuatro saltos para acceder a las terminales a través de las tablas de rutas programadas en los equipos. También se comprobó el correcto funcionamiento de las acciones de control (escritura de registros internos de memoria, entradas y salidas de los módulos), las acciones de gestión de red (manejo de rutas y alarmas provenientes de fallas de la red), las alarmas provenientes de eventos generados por el sistema y las funciones especiales (como lectura del estado de la batería, algoritmo de prueba, reinicio de los módulos, cambios de canal y dirección y respaldo de la memoria de datos en EEPROM interna). Todo eso sobre todos los módulos presentes en la red de nivel superior ‘en caliente’.

Por su parte, el CCGR se programó para interrogar todos los módulos. En la prueba de la red prototipo, se activaron las cargas remotas a través de los actuadores y se comprobó la efectividad en la detección de eventos por parte de los sensores.

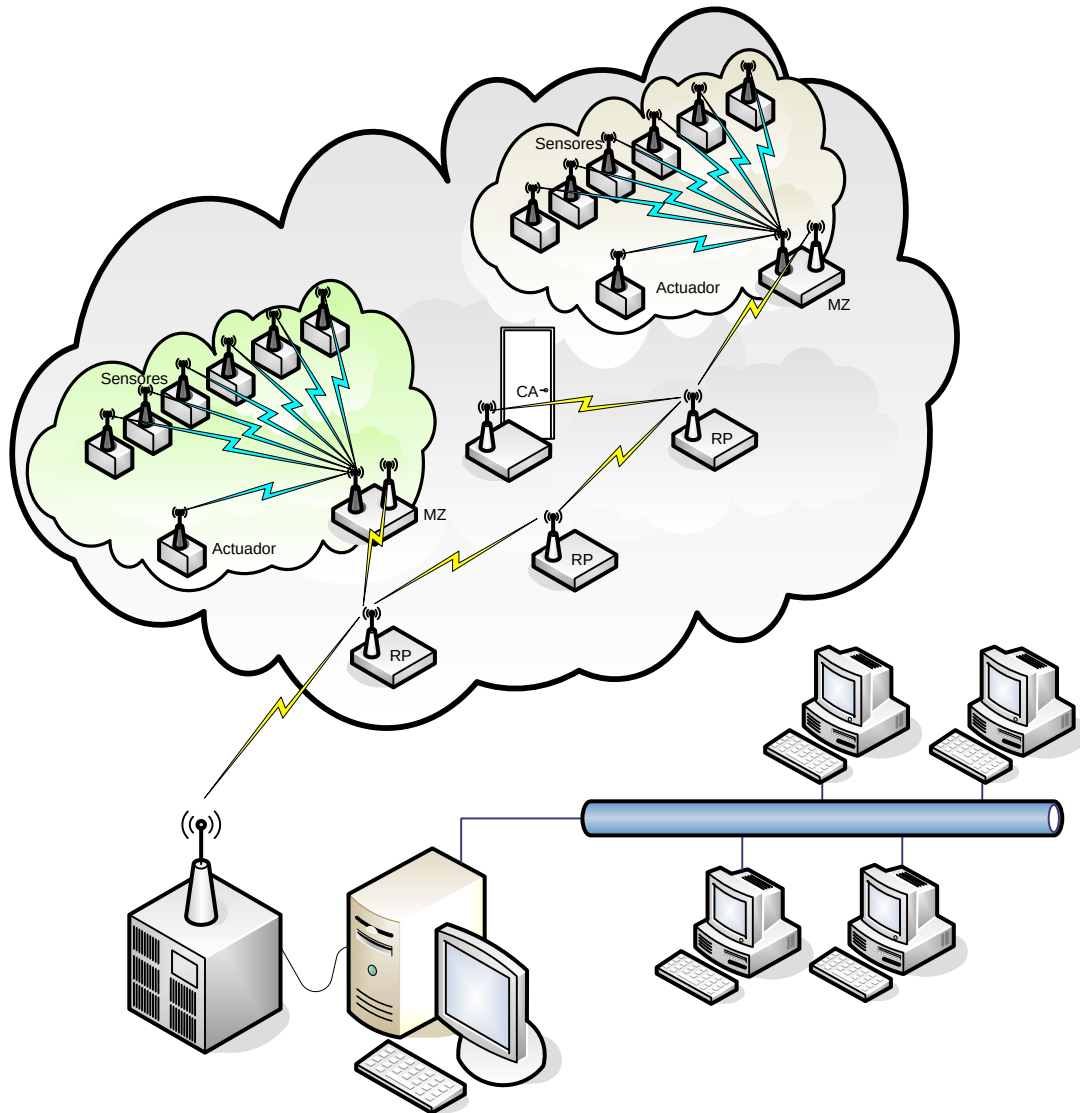


Figura 42. Sistema prototipo montado en la EIE de la UCV

A través de estas pruebas, y una vez realizadas las correcciones menores pertinentes, se verificó que el desempeño de la red siempre estuvo dentro de lo esperado. También se determinó que la efectividad del enlace no siempre es un

parámetro constante en el sistema, ya que ésta depende de muchos factores externos como la temperatura, la humedad, la posición de cuerpos circundantes, entre otros. Sin embargo, el uso del algoritmo de pruebas para determinar la efectividad entre los enlaces siempre permitió encontrar el mejor canal y dirección para integrar un equipo a la red. Los módulos transceptores en la banda de 2.4 GHz tuvieron un alcance (dentro del edificio de la EIE de la UCV) de entre 30 y 40 metros.

RECOMENDACIONES

Como todo sistema, éste es susceptible a mejoras y perfeccionamientos. En opinión del autor, algunas de las mejoras que podrían practicarse son:

1. Desarrollar los mismos módulos del sistema en tecnología de montaje superficial, con lo cual se conseguiría reducir sensiblemente el tamaño, el costo, y posiblemente el consumo de potencia de los mismos. Ya que esta tecnología no se maneja actualmente en los laboratorios de electrónica de la EIE de la UCV, se recomienda la incorporación de nuevas tecnologías en el área de circuitos impresos para construir prototipos, para alinearse con las tendencias actuales en el área de la electrónica.
2. Incorporar módulos sensores y actuadores para otros usos, diferentes a los que han sido diseñados en el presente trabajo.
3. Desarrollar un transceptor en 2.4 GHz basado en el mismo circuito integrado que emplean los módulos TRF24G, a saber el chip NRF2401 de Nordic o uno más avanzado en prestaciones, aumentando el nivel de potencia de salida e incorporando una antena tipo dipolo vertical para lograr un patrón de radiación menos direccional. Con ello no sólo se conseguiría mejorar el sistema, sino reducir sus costos sensiblemente.
4. Determinar el tiempo de autonomía de las baterías en cada módulo, atendiendo a la configuración y tráfico de datos en cada uno de los dispositivos.

CONCLUSIONES

1. El uso de un sistema inalámbrico abarata los costos de instalación, mantenimiento y desinstalación, ya que no se requiere de obras para canalización del cableado, lo cual lo hace más rápido y sencillo. Adicionalmente, le confiere mayor seguridad al sistema, ya que no se puede inhabilitar mediante el corte de cables y además se requiere el manejo de ciertas tecnologías inalámbricas para atacar el sistema.
2. Aunque el sistema no se diseñó con perspectivas a ser un sistema de control de edificaciones, permite la utilización de actuadores inalámbricos para el manejo de cargas.
3. El sistema, gracias al respaldo de energía por batería que todos los módulos tienen, es completamente independiente del suministro eléctrico de la edificación, durante un período de tiempo de autonomía para cada módulo.
4. Gracias al uso de identificadores de zona en cada sensor inalámbrico, no hay peligro de que los mensajes de alarma provenientes de una zona sean procesados por el MZ de otra zona adyacente que opere en la misma banda de frecuencia.
5. La modalidad de detección de “nuevo dispositivo detectado” manejado como una alarma de forma automática al aparecer un dispositivo nuevo no configurado en la red de nivel inferior, confiere al sistema mayor facilidad de instalación y manejo.

6. El uso de transmisores solamente en los sensores y receptores únicamente en los actuadores del sistema permitió reducir sensiblemente el costo de dichos módulos y finalmente el costo general del sistema.
7. El uso del transceptor TRF-2.4G de Laipac Technology Inc. reportó amplias ventajas, ya que sus dimensiones son muy reducidas y posee la antena incorporada, lo cual ofrece un alcance muy direccional bastante considerable (unos 250 metros en líneas de vista y de 30 a 40 metros dentro de la edificación). Adicionalmente, ya que posee 125 canales disponibles, es posible armar hasta 62 sistemas similares, lo cual permitiría implementarlo en edificios de dimensiones mucho mayores que la EIE de la UCV.
8. El uso de transmisores (TLPXXXA)³¹ y receptores (RLPXXXA)³² tuvo la dificultad de que fue necesario programar la codificación, el cálculo de errores, el empaquetamiento de datos y el sistema de transferencia de transmisión y recepción de datos; ya que estos módulos solo hacen el trabajo de modulación y demodulación. Sin embargo, dado que se usaron antenas tipo dipolo vertical de un cuarto de la longitud de onda, lo cual confería un patrón de radiación de potencia isotrópico a los módulos, fue posible armar redes de nivel inferior en estrella alrededor del MZ con un buen alcance (unos 100 m a través de paredes).
9. La incorporación de un sistema de autoprotección en todos los módulos del sistema³³, confiere mayor seguridad al mismo.
10. El hecho de que el sistema posea una arquitectura de árbol de ramales entrelazados en el nivel superior de red, hace que éste sea más sólido y seguro, puesto que los datos que viajan en la red tienen la posibilidad de llegar

³¹ TLP315A, TLP418A y TLP434A

³² RLP315A, RLP418A y RLP434A

³³ Excepto los actuadores, ya que no tienen transmisor.

a su destino a través de múltiples rutas. Adicionalmente, esto soluciona el problema de la instalación de componentes muy alejados.

BIBLIOGRAFÍAS

Tesis

Ortega M., Camilo R. Diseño de un sistema de seguridad inalámbrico para uso en residencias unifamiliares / Camilo Ortega (Tesis).__ Caracas: Universidad Central de Venezuela, 2003.

Zamorano A., Roberto E. Sistema de seguridad inalámbrico, programable con auto chequeo / Roberto Zamorano (Tesis).__ Caracas: Universidad Central de Venezuela, 2003.

Normas

Covenin (823:2002). Guía instructiva sobre sistemas de detección, alarma y extinción de incendios (1ª revisión).__ Caracas: Comisión Venezolana de Normas Industriales. Fondonorma.-- 21 p.

Entrevistas

Entrevista realizada al Ingeniero Freddy Brito (Director de la Escuela de Ingeniería Eléctrica) en la Escuela de Ingeniería Eléctrica. U.C.V., julio 2006

Internet

Productos ADEMCO <[http:// www.ademco.com](http://www.ademco.com)> [Consulta: 2005]

Productos Caddx de GE <[http:// www.caddx.com](http://www.caddx.com)> [Consulta: 2005]

Casadomo Soluciones S.L. Página de domótica y hogar digital <[http:// www.casadomo.com](http://www.casadomo.com)> [Consulta: 2005]

Página informativa, de productos y servicios. <[http:// www.domocode.com](http://www.domocode.com)> [Consulta: 2005]

Productos domótica Viva S.L. <[http:// www.domoticaviva.com](http://www.domoticaviva.com)> [Consulta: 2005]

Productos GE <[http:// www.geindustrial.com](http://www.geindustrial.com)> [Consulta: 2005]

Página informativa, de productos y servicios. <[http:// www.iceseguridad.com](http://www.iceseguridad.com)> [Consulta: 2005]

Productos Laipac <[http:// www.laipac.com](http://www.laipac.com)> [Consulta: 2005]

Productos Paradox <[http:// www.paradox.ca](http://www.paradox.ca)> [Consulta: 2005]

Productos Protection One <[http:// www.protectionone.com](http://www.protectionone.com).ve> [Consulta: 2006]

Productos Rokonet. <[http:// www.rokonet.com](http://www.rokonet.com)> [Consulta: 2005]

Productos GE Security Pro <[http:// www.securitypro.com](http://www.securitypro.com)> [Consulta: 2005]

Productos Sovica <[http:// www.sovica.com](http://www.sovica.com).ve> [Consulta: 2006]

Manuales

Manual de Referencia: TRF-2.4G Transceiver Data Sheet. Laipac Technology Inc. Canada S/F. __ 29 p.

Manual de Referencia: Revision (1.1). Single Chip 2.4 GHz Transceiver nRF2401. Product Specification. Nordic Semiconductor. Noruega, 2004.__39 p.

Manual de Referencia: TLP434A & RLP434A. RF ASK hibrid modules for radio control (New version). Laipac Technology Inc. Canada S/F. __ 1 p.

Manual de Referencia: PIC12F683 Data Sheet. Microchip Technology Inc. EUA 2004.__ 146 p.

Manual de Referencia: PIC18F2525/2620/4525/4620 Data Sheet. Microchip Technology Inc. EUA 2004.__ 146 p.

Manual de Referencia: Versión (1.1a). ModBus Application Protocol Specification. Modbus IDA. EUA 2004.__ 51p.

[ANEXO N° 1]

[Diagrama esquemático y de circuito impreso del módulo MZ]

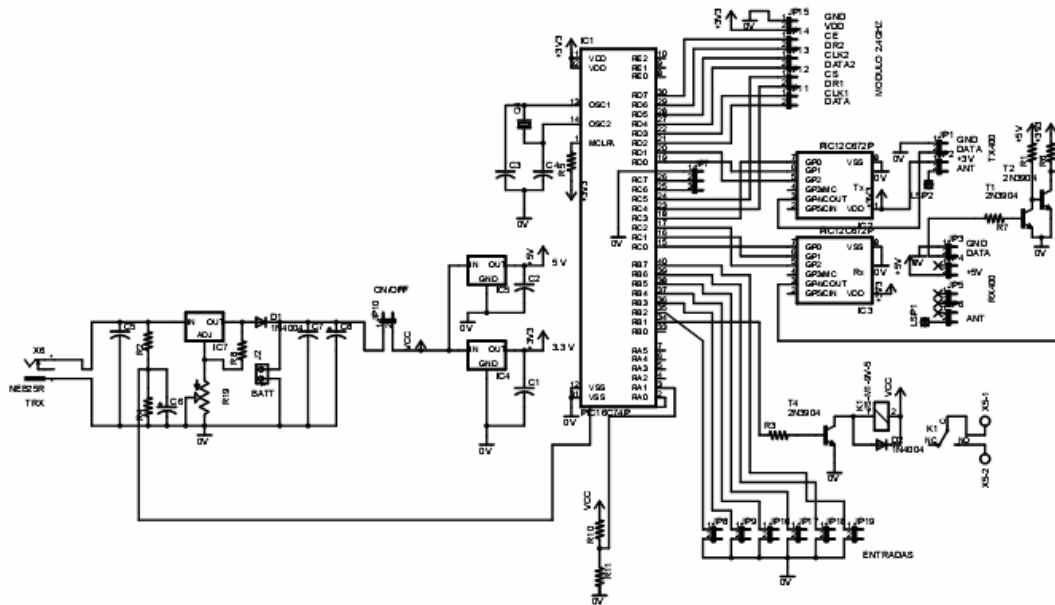
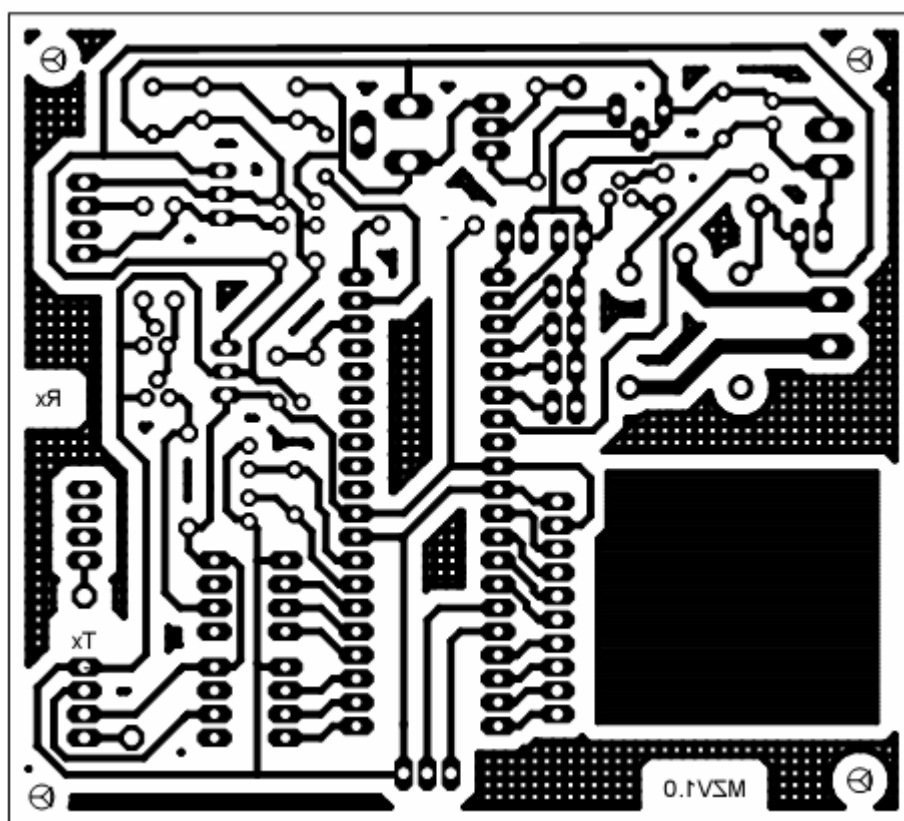


Diagrama esquemático del módulo MZ

[ANEXO N° 1]

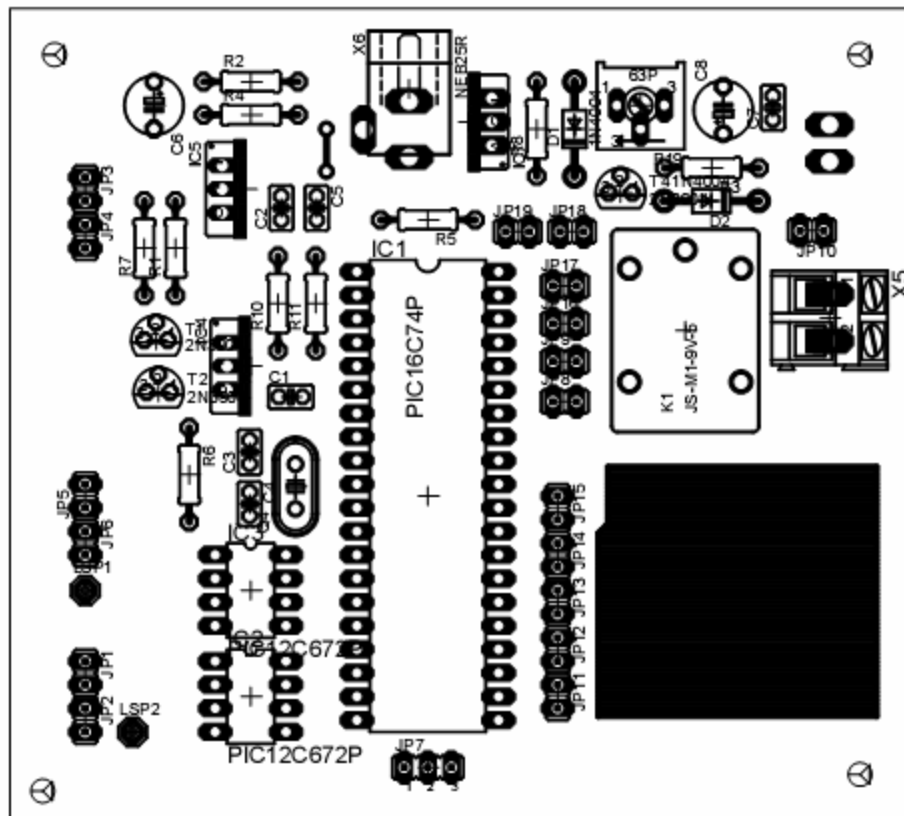
[Diagrama esquemático y de circuito impreso del módulo MZ]



Circuito impreso del módulo MZ

[ANEXO N° 1]

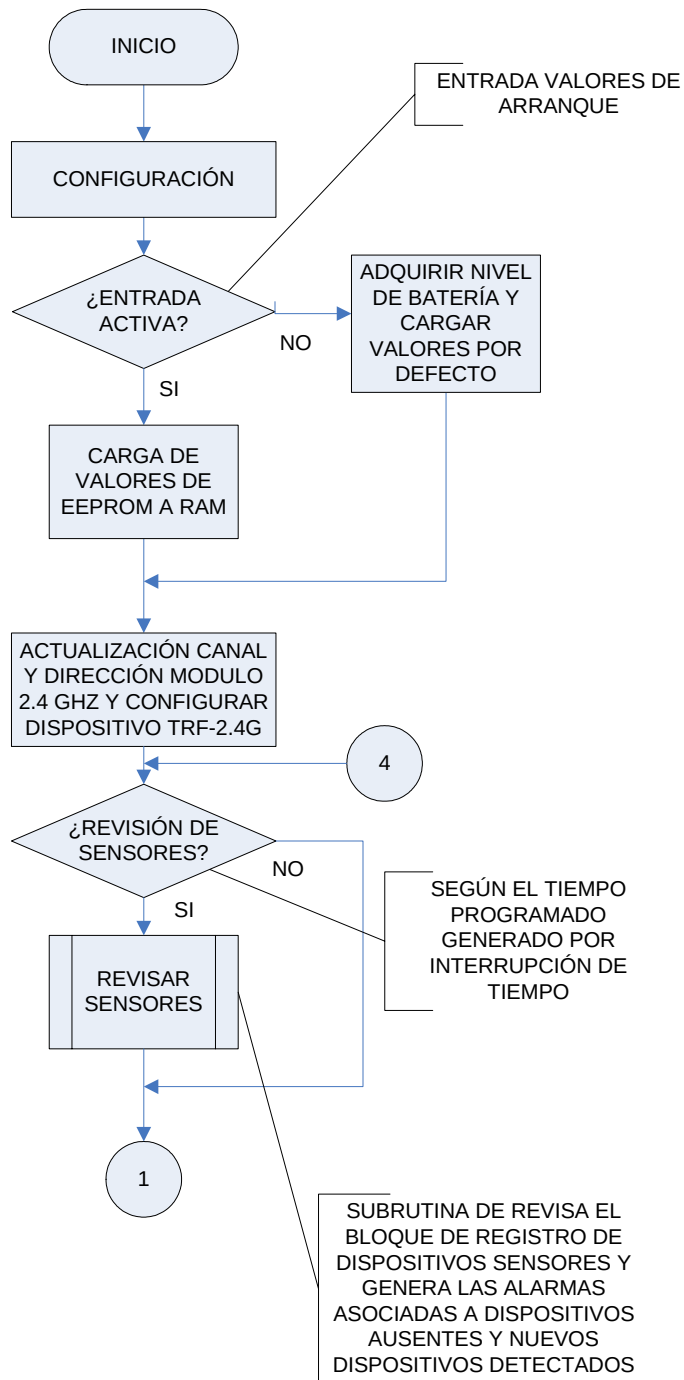
[Diagrama esquemático y de circuito impreso del módulo MZ]



Cara de componentes del módulo MZ

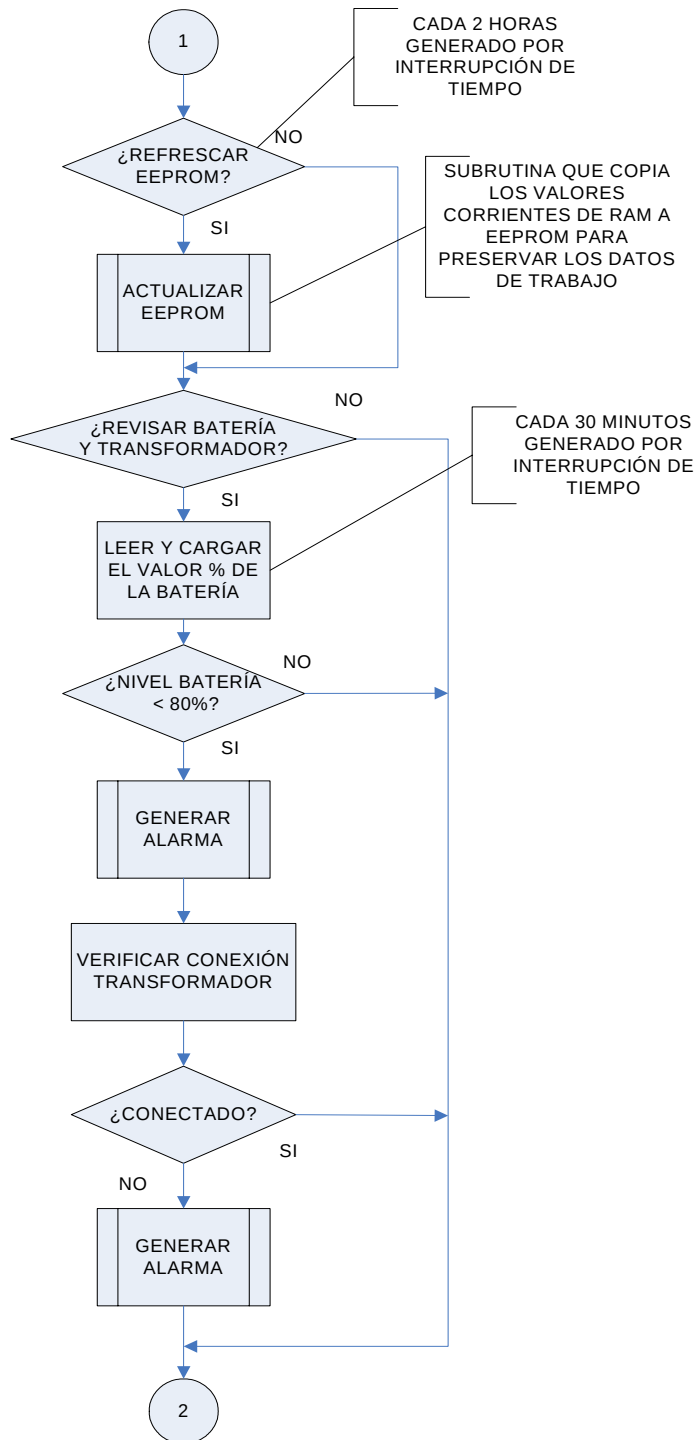
[ANEXO N° 2]

[Diagramas de flujo de la operación del módulo MZ]



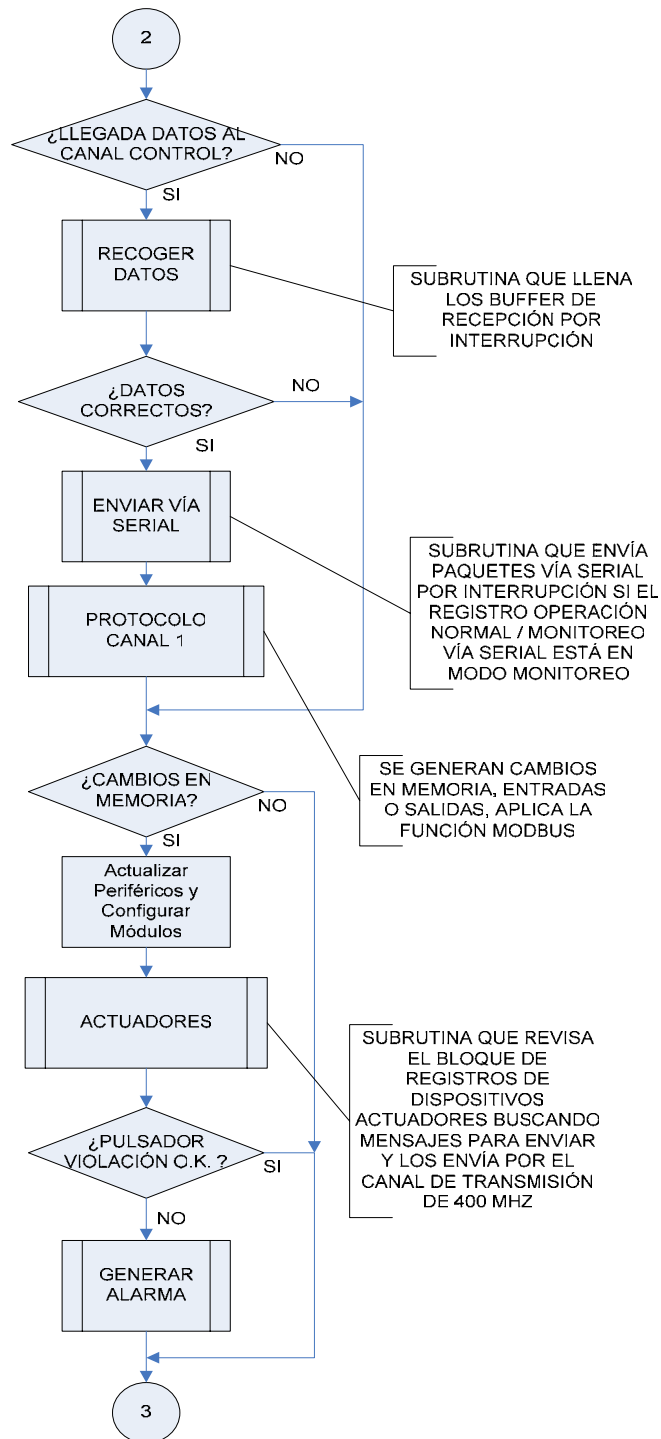
[ANEXO N° 2]

[Diagramas de flujo de la operación del módulo MZ]



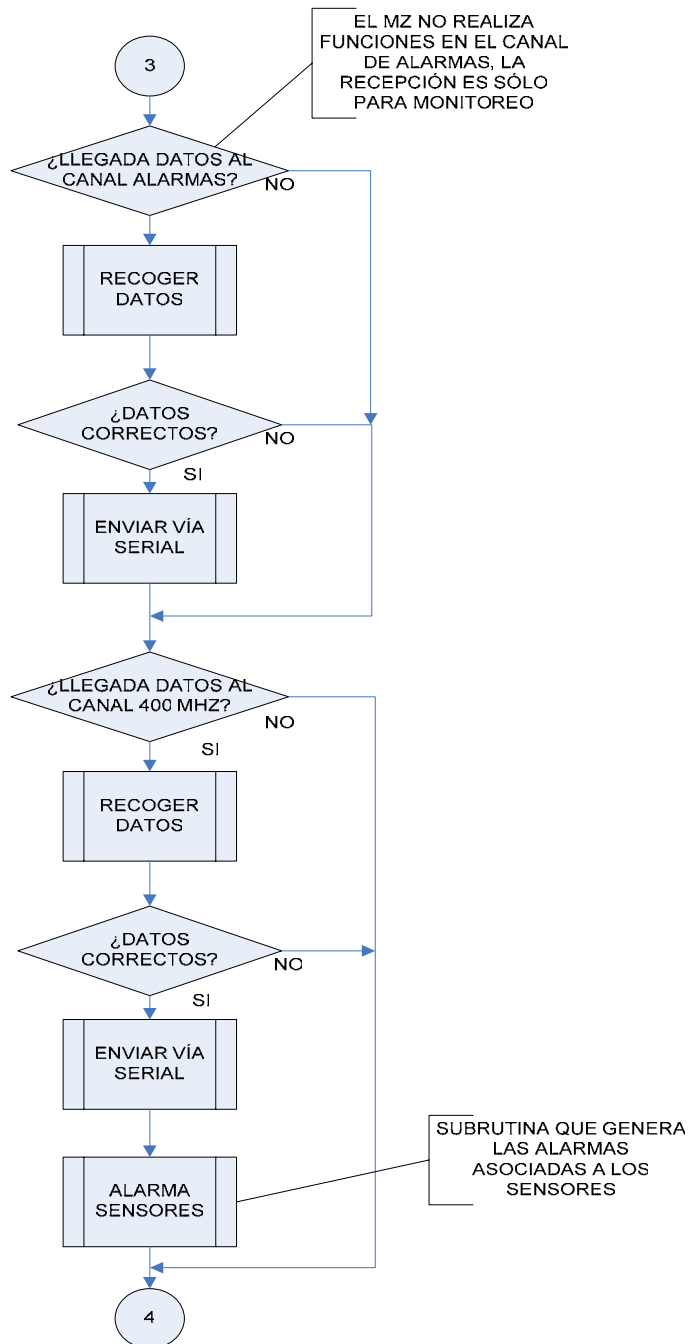
[ANEXO N° 2]

[Diagramas de flujo de la operación del módulo MZ]



[ANEXO N° 2]

[Diagramas de flujo de la operación del módulo MZ]



[Diagrama esquemático y de circuito impreso del módulo RP]

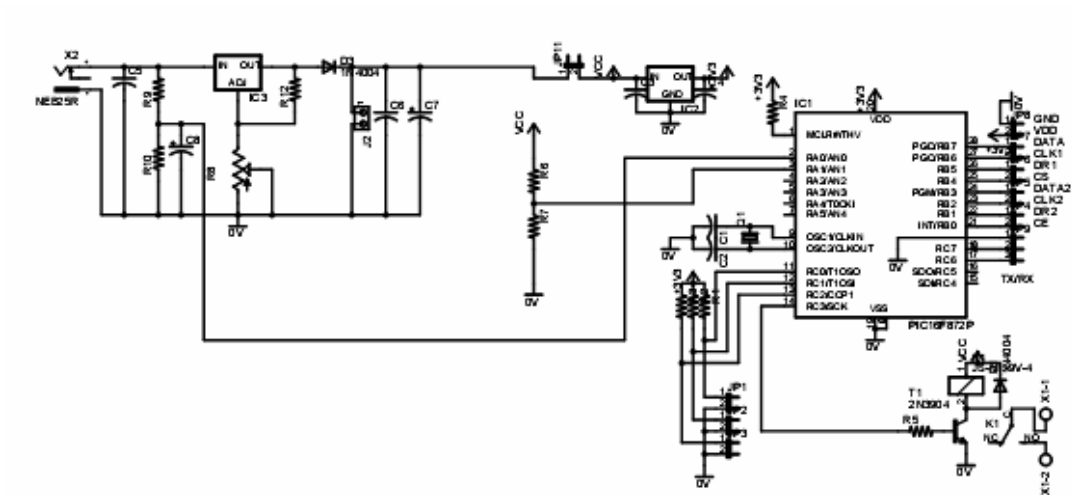
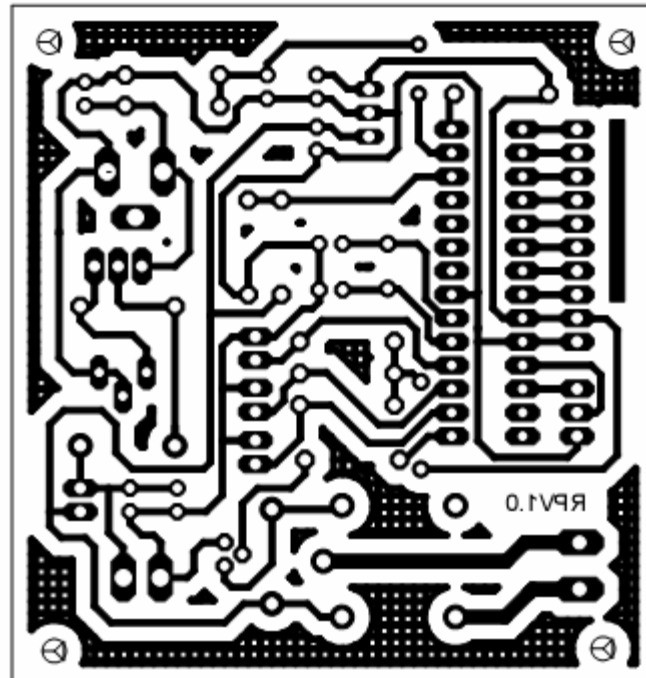


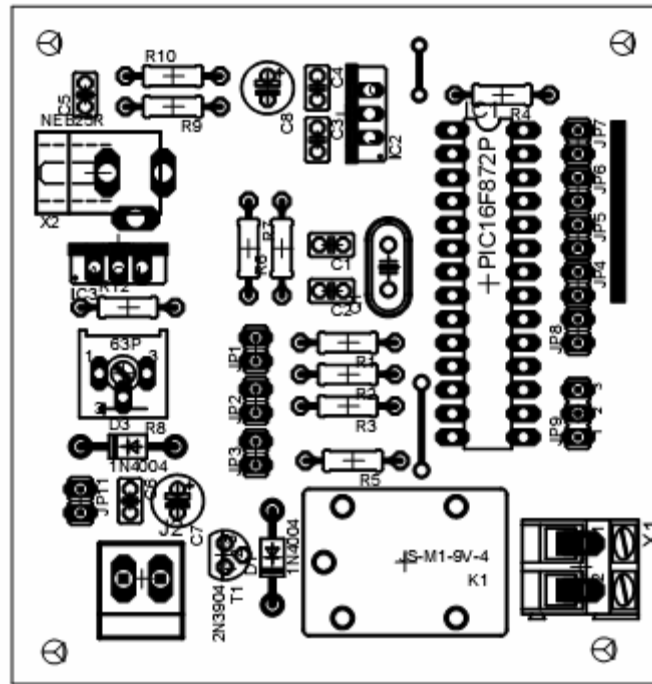
Diagrama esquemático del módulo RP



Circuito impreso del módulo RP

[ANEXO N° 3]

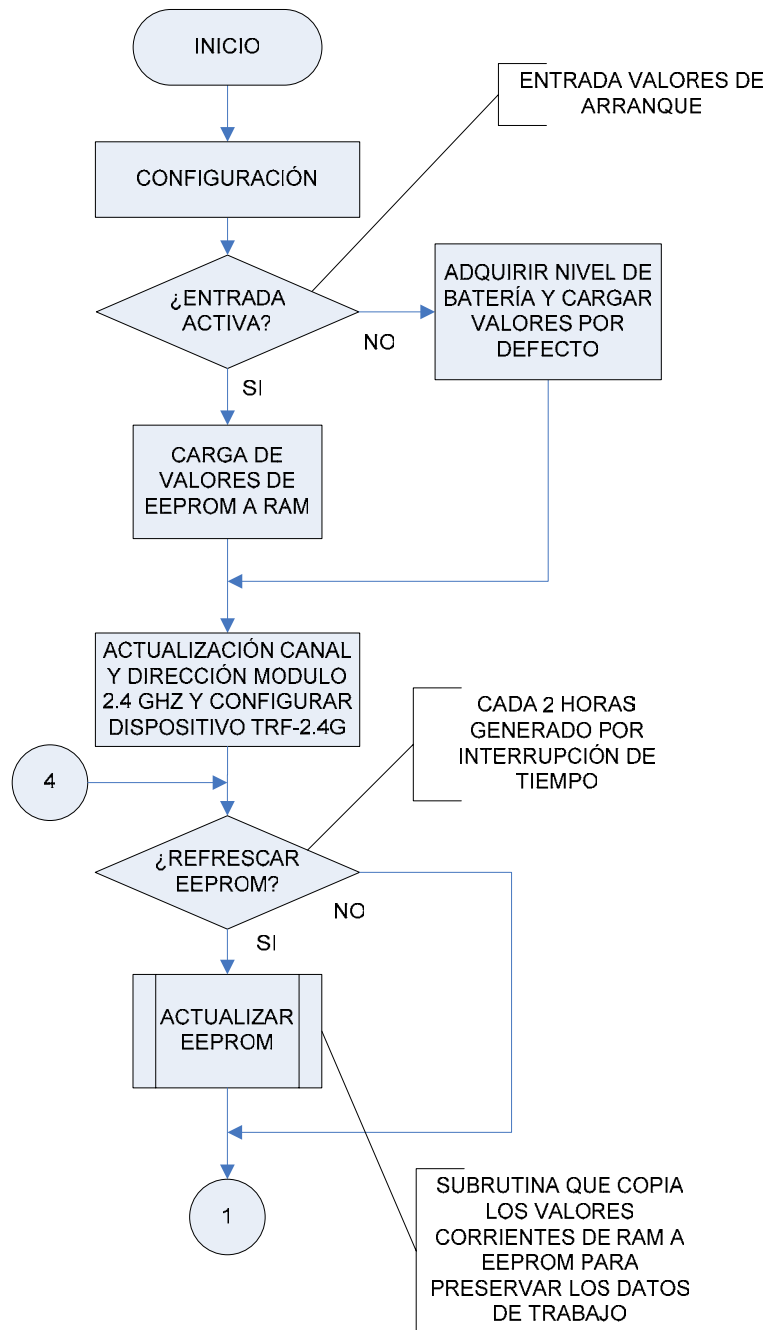
[Diagrama esquemático y de circuito impreso del módulo RP]



Cara de componentes del módulo RP

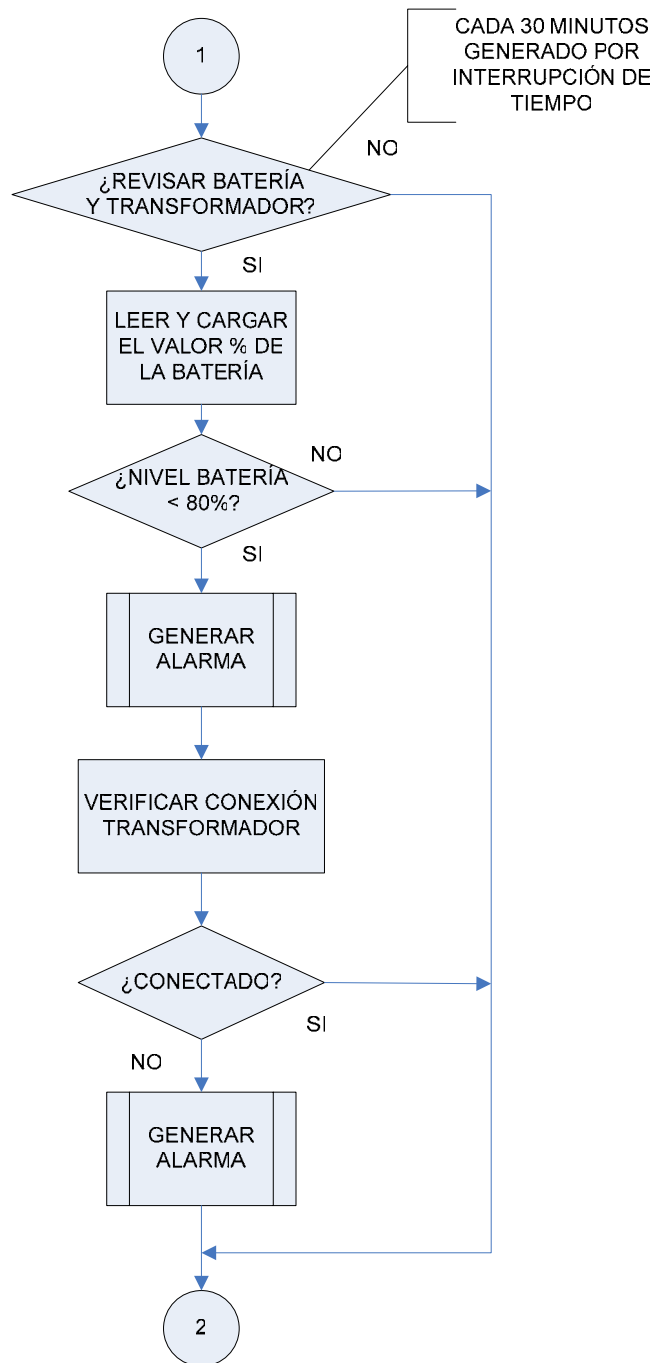
[ANEXO N° 4]

[Diagramas de flujo de la operación del módulo RP]



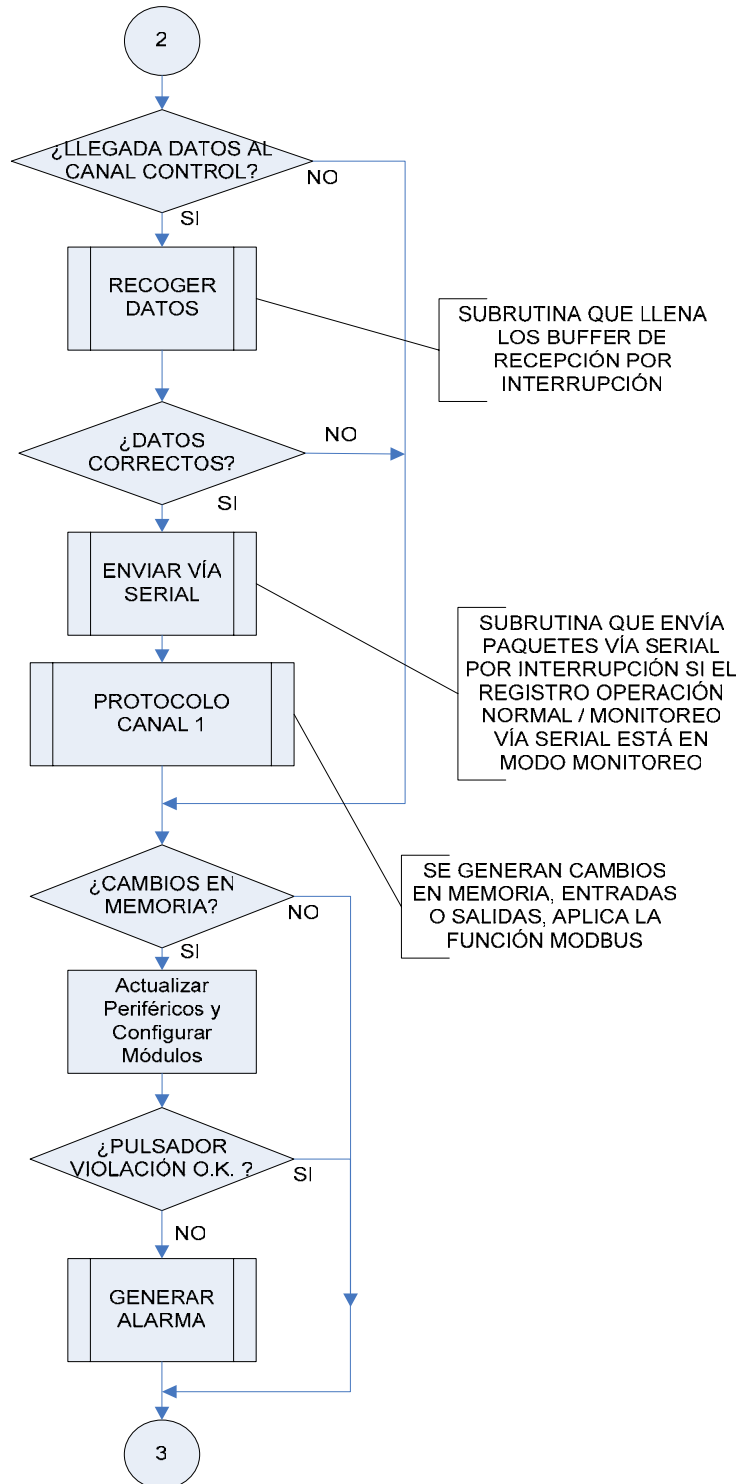
[ANEXO N° 4]

[Diagramas de flujo de la operación del módulo RP]



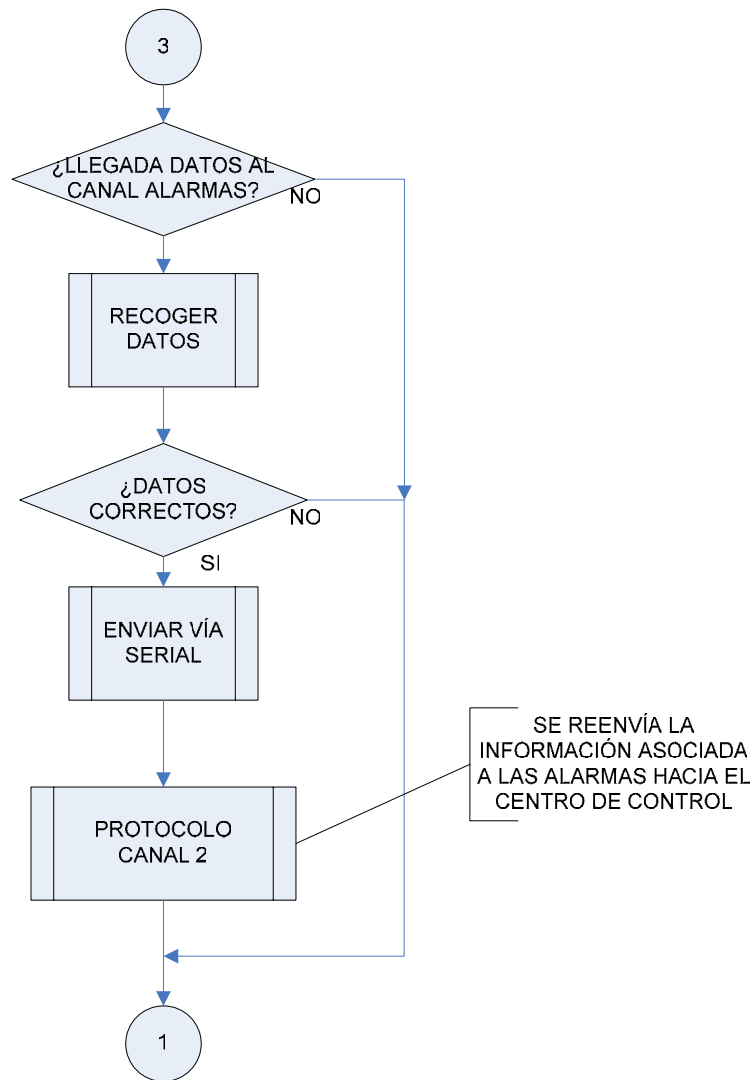
[ANEXO N° 4]

[Diagramas de flujo de la operación del módulo RP]



[ANEXO N° 4]

[Diagramas de flujo de la operación del módulo RP]



[Diagrama esquemático y de circuito impreso del módulo CA]

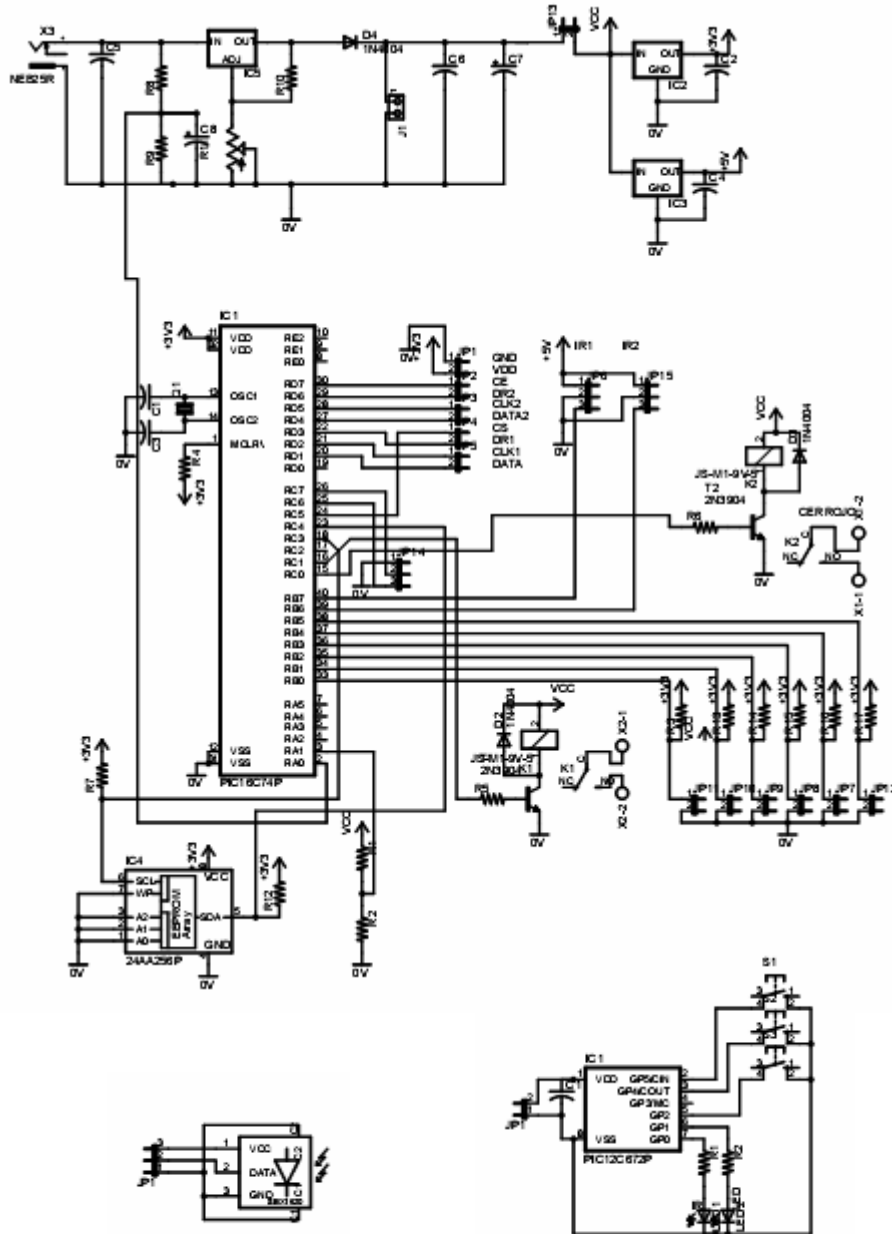
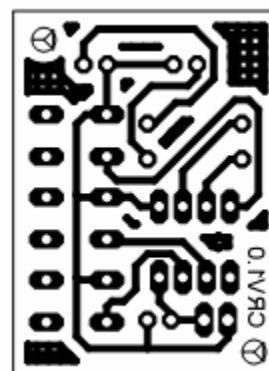
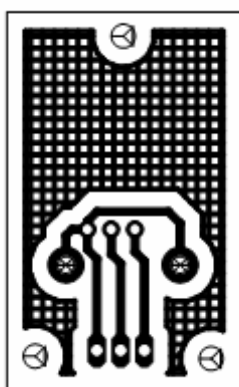
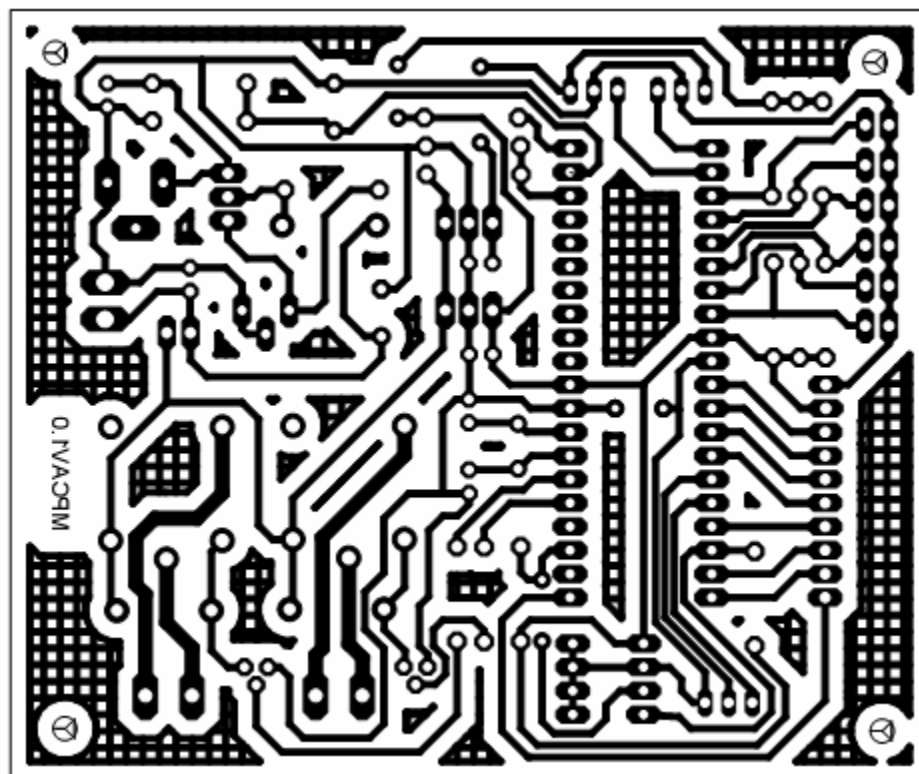


Diagrama esquemático del módulo CA (principal, detector infrarrojo y control remoto)

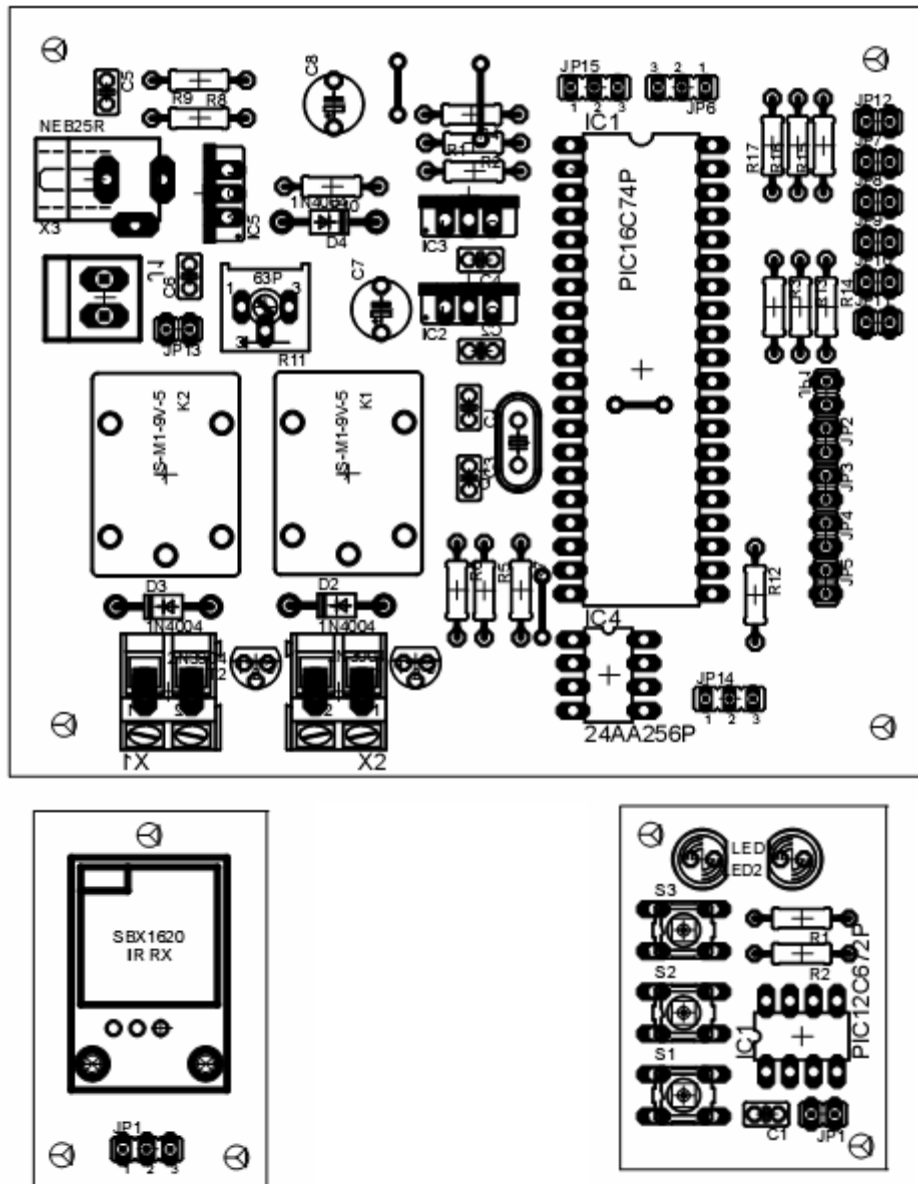
[ANEXO N° 5]

[Diagrama esquemático y de circuito impreso del módulo CA]



Circuito impreso del módulo CA (principal, detector infrarrojo y control remoto)

[Diagrama esquemático y de circuito impreso del módulo CA]



Cara de componentes del módulo CA (principal, detector infrarrojo y control remoto)

[ANEXO N° 6]

[Ejemplos de funcionamiento de registros de gestión de usuarios en CA]

Ejemplo 1. Lectura de la clave del usuario número 1528 (ver figura A6-1).

1.- Al realizar una lectura del bloque de Gestión de Usuarios el campo ‘Estado de la Operación’ indica que el sistema está en espera (no hay ninguna operación en curso).

2.- Se escribe el código de Escuela, el código de Facultad y el número de usuario en los campos correspondientes y 0000 h en el campo ‘LEER / ESCRIBIR’, ‘CLAVE DE USUARIO’, ‘ESTADO DE LA OPERACIÓN’ y ‘ESTADO DEL USUARIO’.

3.- Una vez que el CCGR verifique que el registro ‘ESTADO DE LA OPERACIÓN’ indica proceso de lectura completo, puede leer la clave de usuario y su estado desde los registros correspondientes.

	1	2	3
CÓDIGO DE ESCUELA	0000	XXXX	0000
CÓDIGO DE FACULTAD	0000	XXXX	0000
LEER / ESCRIBIR	0000	0000	0000
NÚMERO DE USUARIO	0000	05F8	05F8
CLAVE DE USUARIO	0000	0000	XXXX
ESTADO DE LA OPERACIÓN	0000	0000	0004
ESTADO DEL USUARIO	0000	0000	XXXX
USO NO DEFINIDO	0000	0000	0000

Figura A6-1. Proceso de lectura de la clave de un usuario

[ANEXO N° 6]

[Ejemplos de funcionamiento de registros de gestión de usuarios en CA]

Ejemplo 2. Escritura de la clave del usuario número 1528 (ver figura A6-2).

1.- Al realizar una lectura del bloque de Gestión de Usuarios el campo ‘Estado de la Operación’ indica que el sistema está en espera (no hay ninguna operación en curso).

2.- Se escribe el código de Escuela, el código de Facultad, el número y clave de usuario en los campos correspondientes, FFFF h en el campo ‘LEER / ESCRIBIR’ y 0000 h en los registros ‘ESTADO DE LA OPERACIÓN’ y ‘ESTADO DEL USUARIO’ (para eliminar a un usuario, basta con escribir 0000 h en el campo ‘CLAVE DE USUARIO’).

3.- Una vez que el CCGR verifique que el registro ‘ESTADO DE LA OPERACIÓN’ indica proceso de escritura completo, el usuario ya habrá sido ingresado a la memoria interna.

	1	2	3
CÓDIGO DE ESCUELA	0000	XXXX	0000
CÓDIGO DE FACULTAD	0000	XXXX	0000
LEER / ESCRIBIR	0000	FFFF	0000
NÚMERO DE USUARIO	0000	05F8	05F8
CLAVE DE USUARIO	0000	XXXX	XXXX
ESTADO DE LA OPERACIÓN	0000	0000	0003
ESTADO DEL USUARIO	0000	0000	XXXX
USO NO DEFINIDO	0000	0000	0000

Figura A6-2. Proceso de escritura de la clave de un usuario

[ANEXO N° 7]

[Diagrama esquemático y de circuito impreso del módulo sensor]

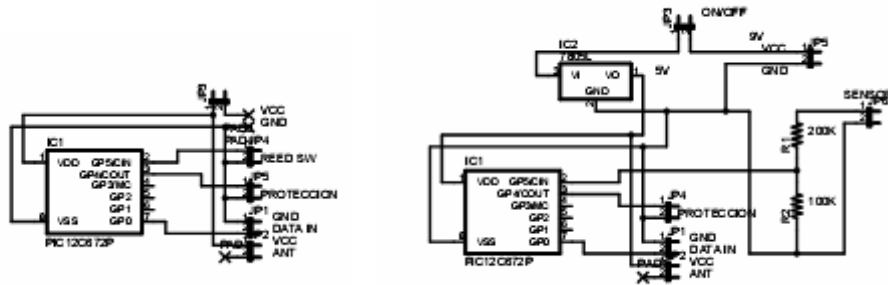
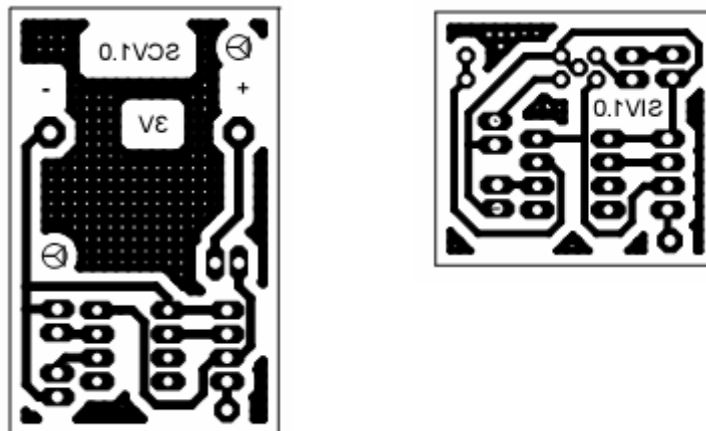


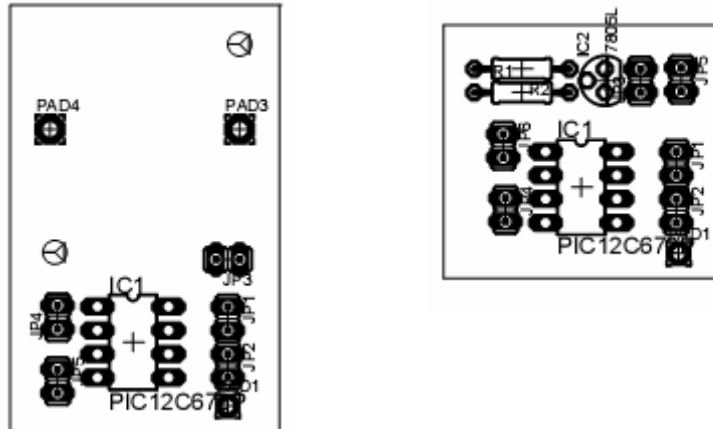
Diagrama esquemático de módulos sensores (de contacto y para detector de incendio)



Circuito impreso de módulos sensores (de contacto y para detector de incendio)

[ANEXO N° 7]

[Diagrama esquemático y de circuito impreso del módulo sensor]



Cara de componentes de módulos sensores (de contacto y para detector de incendio)

[Diagrama esquemático y de circuito impreso del módulo actuador]

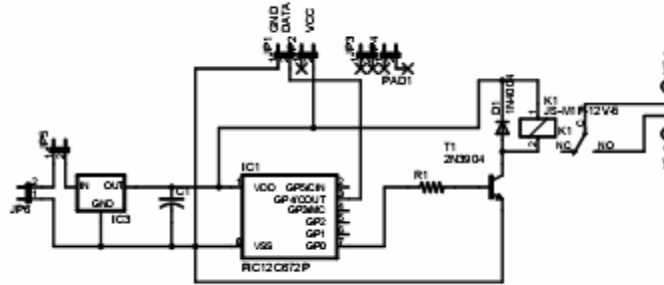
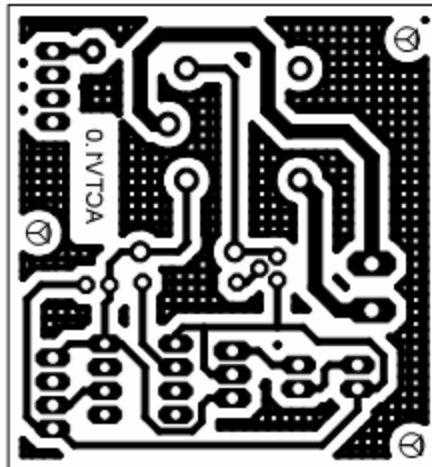


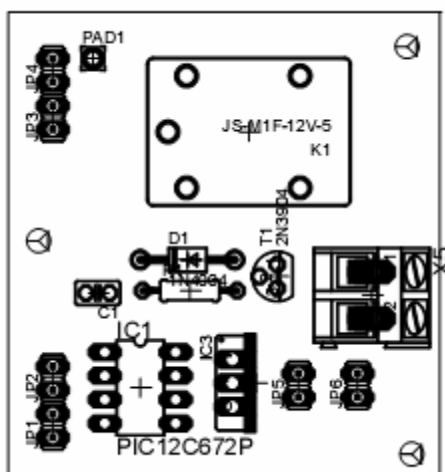
Diagrama esquemático de módulos actuadores



Circuito impreso de módulos actuadores

[ANEXO N° 8]

[Diagrama esquemático y de circuito impreso del módulo actuador]



Cara de componentes de módulos actuadores

[ANEXO N° 9]

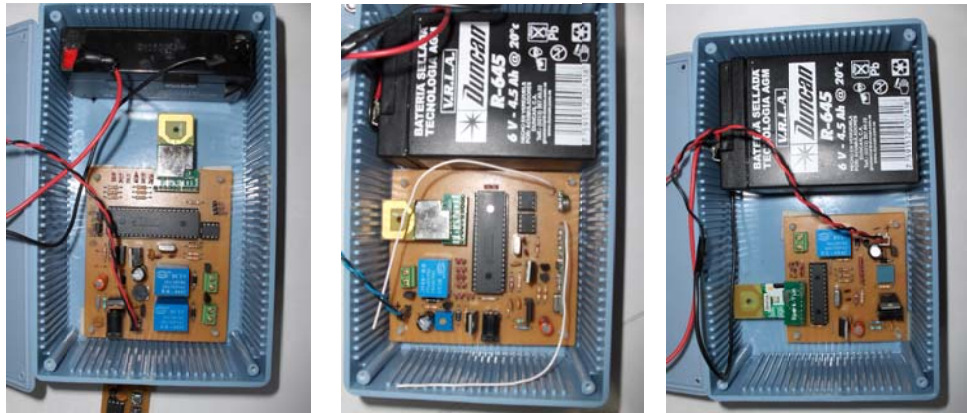
[Fotografía de los equipos desarrollados en el presente trabajo]



Vista general de todos los equipos prototipo del sistema. Los equipos de caja azul pertenecen a la red de nivel superior. Los demás, son de la red de nivel inferior (a excepción del equipo que no posee caja, el cual es el CCGR desarrollado en el Trabajo de grado “Sistema de Control Maestro para el Sistema de Seguridad Inalámbrico de la EIE de la UCV”, presentado por el Br. José Carrasquel).

[ANEXO N° 9]

[Fotografía de los equipos desarrollados en el presente trabajo]



Control de Acceso, Maestro de Zona y Repetidora



Sensor de incendio y sensor de presencia



Sensor de vibración, sensor de apertura y actuador con salida a relé