TRABAJO ESPECIAL DE GRADO

DISEÑO E IMPLEMENTACIÓN DE UN PROTOCOLO DE COMUNICACIONES PARA EL SISTEMA DE SEGURIDAD INALÁMBRICO DE LA ESCUELA DE INGENIERÍA ELÉCTRICA DE LA UCV

Presentado ante la Ilustre
Universidad Central de Venezuela
Por el Br.: Roa P., Boris A.
para optar al Título de
Ingeniero Electricista

Caracas, 2006

TRABAJO ESPECIAL DE GRADO

DISEÑO E IMPLEMENTACIÓN DE UN PROTOCOLO DE COMUNICACIONES PARA EL SISTEMA DE SEGURIDAD INALÁMBRICO DE LA ESCUELA DE INGENIERÍA ELÉCTRICA DE LA UCV

Tutor Académico: Prof. Freddy Brito

Presentado ante la Ilustre
Universidad Central de Venezuela
Por el Br.: Roa P., Boris A.
para optar al Título de
Ingeniero Electricista

Caracas, 2006

UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERIA
ESCUELA DE INGENIERIA ELECTRICA
DEPARTAMENTO DE COMUNICACIONES

CONSTANCIA DE APROBACIÓN

Caracas, 14 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 Boris A. Roa P., titulado:

"DISEÑO E IMPLEMENTACIÓN DE UN PROTOCOLO DE COMUNICACIONES PARA EL SISTEMA DE SEGURIDAD INALÁMBRICO DE LA ESCUELA DE INGENIERÍA ELÉCTRICA DE LA UCV"

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

Prof. Zeldivar Bruzual
Jurado

Prof. José Alonso
Jurado

Prof. Freddy Brito
Tutor Académico

Edificio Escuela de Ingeniería Eléctrica, piso 1, oficina 201, Ciudad Universitaria, Los Chaguaramos, Caracas 1051, D.F.
TELÉFONOS. (VOZ) +58 212 6053300 (FAX) +58 212 6053105
Mail: eie-com@elecrisc.ing.ucv.ve

DEDICATORIA

A la constancia y perseverancia de todos estos años y
a mi madre por su amor y paciencia.

Boris A. Roa P.

AGRADECIMIENTOS

A Dios, energía vital sin la cual nada es posible, porque sino no estaría aquí

A mi madre, por su paciencia, su amor y por siempre estar allí

A mis amigos, porque de una u otra forma siempre me han alentado a seguir

A mis compañeros de proyecto Albert Chávez y José Carrasquel, pues el equipo que formamos fue excelente

A Jeniret Vegas por ser tan especial y brindarme tanto apoyo y amor durante este tiempo

Boris A. Roa P.

DISEÑO E IMPLEMENTACIÓN DE UN PROTOCOLO DE COMUNICACIONES PARA EL SISTEMA DE SEGURIDAD INALÁMBRICO DE LA ESCUELA DE INGENIERÍA ELÉCTRICA DE LA UCV

Tutor Académico: Freddy Brito. Tesis. Caracas. U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Ingeniero Electricista. Opción: Comunicaciones. Institución: U.C.V. 2006. 45h. + anexos.

Palabras Claves: Protocolo de comunicaciones; comunicaciones inalámbricas; sistema de seguridad

Resumen. Se presenta el desarrollo de un protocolo de comunicaciones para el sistema de seguridad inalámbrico implementado en la Escuela de Ingeniería Eléctrica de la U.C.V. El protocolo desarrollado permite que los diferentes equipos que forman parte del sistema de seguridad se comuniquen informando en todo momento la situación de la edificación y el estado de integridad de los equipos que lo constituyen. El protocolo utiliza algunas de las características y fortalezas de los protocolos de comunicaciones comerciales e industriales de mayor uso en la actualidad, pero la estructura central fue desarrollada en su totalidad con miras a proveer las comunicaciones para el sistema de seguridad inalámbrico. También se presenta la arquitectura para el sistema de seguridad en función de las características de seguridad deseadas y los dispositivos desarrollados. De las pruebas realizadas al protocolo y a los equipos se verifica que funciona correctamente dentro de los parámetros establecidos y que los mensajes llegan sin errores a su destino. Adicionalmente y como valor agregado, el protocolo permite controlar equipos que no sean parte del sistema de seguridad debido que utiliza algunas funciones del protocolo MODBUS dentro de los mensajes que son enviados durante las comunicaciones en la red.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

SIGLAS

UCV	Universidad Central de Venezuela
EIE	Escuela de Ingeniería Eléctrica
IEEE	Institute of Electrical and Electronics Engineers, Inc.
AT&T	American Telephone and Telegraph
ISO	International Standards Organization

INTRODUCCIÓN

Los sistemas de seguridad son un conjunto de equipos y herramientas que interactúan para proteger y resguardar la integridad de los bienes y de las personas; así como el patrimonio de una empresa, institución o, inclusive, el Estado. Entre las aplicaciones de estos sistemas se encuentra la prevención de incendios, detección temprana de intrusos, el permitir acceso a ciertas zonas de interés a un número restringido de personas previamente autorizadas, evitar el hurto y/o daño intencionado de bienes e inmuebles, entre muchas otras.

En la actualidad, se ha desarrollado un gran número de sistemas de seguridad, entre los cuales figura un grupo que se caracteriza por emplear una interfaz aérea para la transmisión de datos. Dichos sistemas presentan, entre sus ventajas, el uso de la tecnología inalámbrica, por lo que no constan de un sistema de cableado que se despliegue por la zona a resguardar; como consecuencia, son vulnerables menos a la posibilidad de dejar sin protección a toda la zona en resguardo, debido al corte de uno de estos cables. Otra de las características de los sistemas de seguridad que utilizan formas inalámbricas de comunicación, es la posibilidad de transmitir grandes volúmenes de información, característica que permite una codificación y encriptación de los datos de los usuarios, haciendo que sea más difícil el poder interferir el sistema directamente en el ámbito de radio frecuencia.

En la actualidad y debido a los continuos cambios de la sociedad y las situaciones de inseguridad que se presentan en el territorio nacional, incluyendo a La Universidad, se ha vuelto una necesidad el que La Escuela de Ingeniería Eléctrica desarrolle un sistema de seguridad que permita resguardar los bienes y equipos con los que se desarrollan las actividades de docencia, investigación y extensión, para así poder mantener el nivel de excelencia académica que la caracteriza.

Por este motivo surge el proyecto: “Sistema de Seguridad para la Escuela de Ingeniería Eléctrica de la U.C.V.”, en el marco de este proyecto se derivan varios trabajos de grado que son:

- “Red inalámbrica para aplicaciones en sistemas de seguridad”, Br. Albert Chávez
- “Sistema de control maestro para el sistema de seguridad inalámbrico de la E.I.E. de la U.C.V.”, Br. José Carrasquel
- “Diseño e implementación de un protocolo de comunicaciones para el sistema de seguridad inalámbrico de la E.I.E. de la U.C.V.”, Br. Boris Roa

Las dos primeras tesis enfocadas al desarrollo de los dispositivos y equipos que conformarán el sistema de seguridad y la presente tesis enfocada a posibilitar las comunicaciones entre los componentes de la red.

El objetivo general de la presente tesis es el desarrollar los protocolos de comunicaciones, la codificación de datos y la arquitectura del sistema de comunicaciones, necesarios para la implementación de un sistema de seguridad inalámbrico en la Escuela de Ingeniería Eléctrica de la U.C.V.

En el capítulo I se definen las características que debe poseer un protocolo de comunicaciones y se hace una revisión del modelo OSI (*Open System Interconection* – Interconexión de Sistemas Abiertos).

En el capítulo II se presenta el desarrollo y la metodología usada para el diseño del protocolo de comunicaciones, así como también los resultados obtenidos de las pruebas realizadas al sistema de seguridad operando con el protocolo desarrollado.

CAPÍTULO I

TEORÍA DE PROTOCOLO

Protocolos de comunicación

Se le llama protocolo de red o protocolo de comunicación al conjunto de reglas que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red. En este contexto, las entidades de las cuales se habla son programas de computadora o autómatas de otro tipo, tales como dispositivos electrónicos capaces de interactuar en una red. Estos protocolos de comunicaciones definen, por ejemplo, los formatos de información que utilizan las computadoras conectadas a una red para la cooperación e intercambio de información. Son ellos, entonces, los que definen la manera como compartimos información a través del Internet, incluso la forma de enviar un correo electrónico.

En la actualidad se cuenta con muchos protocolos de comunicaciones comerciales, incluso algunas empresas de telecomunicaciones tales como la AT&T han llegado a desarrollar sus propios protocolos, en función de los servicios que ofrezcan a sus usuarios. Muchas veces estos protocolos, aún sin que el usuario se de cuenta, son usados para llevar a cabo diversas comunicaciones, a través de Internet, transferencias vía módem o una simple comunicación a un servicio en línea inteligente de algún banco.

Los protocolos de red establecen aspectos tales como:

- Las secuencias posibles de mensajes durante el proceso de la comunicación.
- La sintaxis de los mensajes intercambiados.
- Estrategias para corregir errores en la comunicación.
- Estrategias de seguridad (autenticación, encriptación).

Los protocolos que son implementados en sistemas de comunicaciones que tienen un amplio impacto, suelen convertirse en estándares, debido a que la comunicación e intercambio de información (datos) es un factor fundamental en numerosos sistemas, y para asegurar tal comunicación se vuelve necesario copiar el diseño y funcionamiento a partir del ejemplo preexistente.

Existen consorcios empresariales y organizaciones que tienen como propósito el proponer recomendaciones de estándares que se deben respetar para asegurar la interoperabilidad de los productos. Ejemplo de lo anterior es la IEEE que propone varios estándares para redes físicas.

En el campo de las redes informáticas, los protocolos pueden ser divididos en varias categorías, una de las clasificaciones más estudiada es el modelo OSI (*Open System Interconection* – Interconexión de Sistemas Abiertos) de la organización ISO (*International Organization for Standarization* – Organización Internacional para la Estandarización).

Descripción del modelo de referencia de Interconexión de Sistemas Abiertos

Este modelo está dividido en siete capas, las cuatro capas superiores trabajan con problemas particulares relacionadazos con las aplicaciones, y las tres capas inferiores se encargan de los problemas pertinentes al transporte de los datos. En la tabla 1 se muestran las diferentes capas del modelo OSI.

Tabla 1. Modelo de referencia de Interconexión de Sistemas Abiertos.

Nivel	Nombre
Capa 7	Nivel de aplicación
Capa 6	Nivel de presentación
Capa 5	Nivel de sesión
Capa 4	Nivel de transporte
Capa 3	Nivel de red
Capa 2	Nivel de enlace de datos
Capa 1	Nivel físico

Capa Física

La Capa Física del modelo de referencia OSI es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio (cable conductor, fibra óptica ó RF), características del medio (tipo de cable o calidad del mismo, tipo de conectores normalizados o en su caso tipo de antena, etc.) y la forma en la que se transmite la información (codificación de señal, niveles de tensión/intensidad de corriente eléctrica, modulación, tasa binaria, etc.)

Esta capa se encarga de transmitir los bits de información a través del medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes, de la velocidad de transmisión, si es unidireccional o bidireccional. También de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas o electromagnéticas.

Durante una transmisión de datos, esta capa se encarga de transformar una trama de datos proveniente del nivel de enlace en una señal adecuada al medio físico utilizado en la transmisión. Estas señales pueden ser eléctricas (transmisión por un par de cobre), o electromagnéticas; estas últimas, dependiendo de la frecuencia de la señal pueden ser ópticas, de microondas o de radio. Cuando actúa en modo recepción el trabajo es inverso, se encarga de transformar la señal recibida en tramas de datos binarios que serán entregados al nivel de enlace.

En otras palabras, cuando la capa física recibe una trama binaria, ésta es convertida en una señal electromagnética adaptada al medio físico, de tal forma, que a pesar de la degradación que pueda sufrir en el medio de transmisión, vuelva a ser interpretable correctamente en el receptor.

Topología y medios compartidos

Indirectamente el tipo de conexión que se haga en la capa física puede influir en el diseño de la Capa de Enlace. Atendiendo al número de equipos que comparten un medio hay dos posibilidades:

- Conexiones punto a punto: que se establecen entre dos equipos y que no admiten ser compartidas por terceros
- Conexiones punto-multipunto: en las que dos o más equipos pueden usar el medio.

Así, por ejemplo, la fibra óptica no permite fácilmente conexiones punto-multipunto, por el contrario, las conexiones inalámbricas son inherentemente punto-multipunto. Hay topologías de tipo anillo, que permiten conectar muchas máquinas a partir de una serie de conexiones punto a punto.

La técnica utilizada para lograr que los nodos sobre la red, accedan al cable ó al medio de comunicación y evitar que dos o más estaciones intenten transmitir simultáneamente es trabajo de la Capa de Enlace.

Capa de Enlace

La función de esta capa es la de asegurar la transferencia de datos libres de error entre nodos adyacentes (sincronización a nivel de datos). Debe crear y reconocer los límites de las tramas, así como resolver los problemas derivados del deterioro, pérdida o duplicidad de las tramas. También debe incluir algún mecanismo de regulación del tráfico que evite la saturación de un receptor que sea más lento que el emisor. La capa de enlace de datos está dividida en dos subcapas: la capa MAC (*Media Access Control* - Control de Acceso al Medio) y la capa LLC (*Logical Link Control* - Control de Enlace Lógico). Esta capa se encarga entre otras funciones de definir las estructuras de las tramas, el sincronismo de estas, la detección de errores, el direccionamientos y el control del flujo de las tramas.

Capa de Red

El cometido de esta capa es asegurar que los datos sean llevados desde el origen hasta el destino, aún cuando ambos no estén conectados directamente, es decir, se encarga de encontrar un camino, manteniendo una tabla de rutas que, atravesando todos los equipos que sean necesario, permita hacer llegar los datos a su destino.

Entre las funciones de esta capa se encuentran el control del flujo de datos, la fragmentación y reensamblado de los mensajes, el control de errores y el enrutamiento de los paquetes en la red (selección de rutas).

Adicionalmente la capa de red debe gestionar la congestión de red, que es el fenómeno que se produce cuando una saturación de un nodo tira abajo toda la red.

Capa de Transporte

Su función básica es aceptar los datos enviados por las capas superiores, dividirlos en pequeñas unidades si es necesario, y pasarlos a la capa de red. En el caso del modelo OSI, también se asegura que lleguen correctamente al otro lado de la comunicación. Otra característica a destacar es que debe aislar a las capas superiores de las distintas posibles implementaciones de tecnologías de red en las capas inferiores, lo que la convierte en el corazón de la comunicación. En esta capa se proveen servicios de conexión para la capa de sesión que serán utilizados finalmente por los usuarios de la red al enviar y recibir paquetes. Estos servicios estarán asociados al tipo de comunicación empleada, la cual puede ser diferente según el requerimiento que se le haga a la capa de transporte. Por ejemplo, la comunicación puede ser manejada para que los paquetes sean entregados en el orden exacto en que se enviaron, asegurando una comunicación punto a punto libre de errores, o sin tener en cuenta el orden de envío. Una de las dos modalidades debe establecerse antes de comenzar la comunicación para que una sesión determinada envíe paquetes, y ése será el tipo de servicio brindado por la capa de transporte hasta que la sesión finalice. De la explicación del funcionamiento de esta capa se desprende que no está tan encadenada a capas inferiores como en el caso de las capas 1 a 3, sino que el servicio a prestar se determina cada vez que una sesión desea establecer una comunicación. Todo el servicio que presta la capa está gestionado por las cabeceras que agrega al paquete a transmitir. De esta manera se puede definir a la capa de transporte como: capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la destino, independizándolo del tipo de red física que se esté utilizando.

Capa de Sesión

Esta capa ofrece varios servicios que son cruciales para la comunicación, como son el control de la sesión a establecer entre el emisor y el receptor (quién transmite, quién escucha y seguimiento de ésta), el control de la concurrencia (que dos comunicaciones con la misma operación crítica no se efectúen al mismo tiempo), el mantener puntos de verificación (*checkpoints*), que sirven para que, ante una interrupción de transmisión por cualquier causa, la misma se pueda reanudar desde el último punto de verificación en lugar de repetirla desde el principio.

Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción.

Capa de Presentación

El objetivo de esta capa es la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicote, EBCDIC), números (little-endian tipo Intel, big-endian tipo Motorola), sonido e imágenes; los datos lleguen de manera entendible.

Esta capa es la primera en trabajar más el contenido de la comunicación que en el cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

Por lo tanto, esta capa es la encargada de manejar las estructuras de datos abstractas y realizar las conversiones de representación de datos necesarias para la correcta interpretación de los mismos.

Capa de Aplicación

Ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan dichas aplicaciones para intercambiar datos, como correo electrónico, gestores de bases de datos y servidor de ficheros. Hay tantos protocolos como aplicaciones distintas puesto que continuamente se desarrollan nuevas aplicaciones y el número de protocolos crece constantemente.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación sino con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente. Así, por ejemplo, un usuario no manda una petición "HTTP/1.0 GET index.html" para conseguir una página en html, ni lee directamente el código html/xml.

Hasta aquí casi todas las aplicaciones descritas comparten la arquitectura cliente-servidor, aunque hay otras aplicaciones minoritarias como las redes P2P o los sistemas maestro-esclavo.

En la tabla 2 se muestran algunos protocolos de comunicaciones comerciales, ubicados según la capa del modelo OSI a la que pertenecen.

Tabla 2. Ejemplo de algunos protocolos ubicados según la capa del modelo OSI en la que actúan

Modelo OSI	
Capas	Protocolos
Aplicación	FTAM, X.400, X.500...
Presentación	ASN.1, Videotex, Unicode, MIME, HTML, XML, ...
Sesión	RTSP, H.323, H.248, SIP, RPC, ...
	NetBT, SMB, SSL, TLS, ...
Transporte	TCP, UDP, SCTP, RTP, SPX, TCAP, DCCGRP, ...
Red	NetBEUI, OSPF, ...
Enlace	MPLS, SNA, ...
	Ethernet, Token Ring, LocalTalk, FDDI, X.21, X.25, Frame Relay, BitNet, CAN, ATM, Wi-Fi, HDLC, SDLC, CSMA/CD, CSMA/CA, ...
Física	RS-232, RS-449, EIA-422, EIA-485, V.21-V.23, V.42-V.90,...
	Códigos NRZ, Codificación Manchester, Cable coaxial, Par trenzado,10Base2, 10BASE5, 10BASE-T, 100BASE-TX, PDH, SDH, T-carrier, E-carrier, SONET, DSSS, FHSS, CCGRITT X.211, ISO 10022,...

CAPÍTULO II

PROTOCOLO DE COMUNICACIONES EIE UCV 2006 V.0

Descripción del protocolo

El protocolo desarrollado está diseñado para hacer posible las comunicaciones entre diferentes dispositivos con miras a mantener la seguridad de un recinto; más específicamente, el edificio de la Escuela de Ingeniería Eléctrica de la U.C.V.

En este protocolo se contemplan las comunicaciones entre los dispositivos sensores y los dispositivos concentradores de información por zona, comunicación que se lleva a cabo en la banda de 400MHz, y las comunicaciones entre los concentradores de información por zona, los enrutadores y centro de control y gestión de red, comunicación que sucede en la banda de 2.4GHz.

Entre las cosas que se contempla en el protocolo de comunicaciones están:

- Configuración del sistema de forma remota.
- Sondeo de todos los dispositivos que componen el sistema para determinar su estado e integridad.

- Transmisión de las alarmas que se produzcan en el sistema desde la zona en cuestión hasta el centro de control y gestión de red.
- Manejo de las posibles rutas que deben seguir los diferentes mensajes dentro del sistema para asegurar que lleguen a su destino.
- Generación de alarmas locales y alarmas externas a la edificación.
- Activación de equipos de respaldo en caso de falla de los equipos principales.

Funcionamiento del Protocolo de comunicaciones EIE-2006 V.0

El ***Protocolo EIE-2006 V.0*** está diseñado para realizar las comunicaciones entre los diferentes dispositivos que conforman el sistema de seguridad inalámbrico. Este sistema de seguridad utiliza dos (2) bandas de frecuencia, una para los sensores y otra para el sistema de supervisión, control y transferencia de datos.

La banda que utilizan los sensores está ubicada en 400MHz y la banda para el sistema de supervisión, control y transferencia de datos está ubicada en 2.4GHz. El sistema de supervisión, control y transferencia de datos está compuesto por Maestros de Zona (MZ), Repetidores (RP) y el Centro de Control y Gestión de Red (CCGR). Los MZ poseen transmisores y receptores en la banda de 400MHz ya que deben poder comunicarse con los sensores, pues estos son los que le van a comunicar si existe alguna eventualidad en el edificio.

Primeramente, el edificio de la EIE fue dividido en varias zonas a las cuales se les da el nombre de *Zonas de Seguridad*; en estas zonas están colocados los sensores y maestros de zona. En la ilustración 1 se muestra como están distribuidas dichas zonas de seguridad.

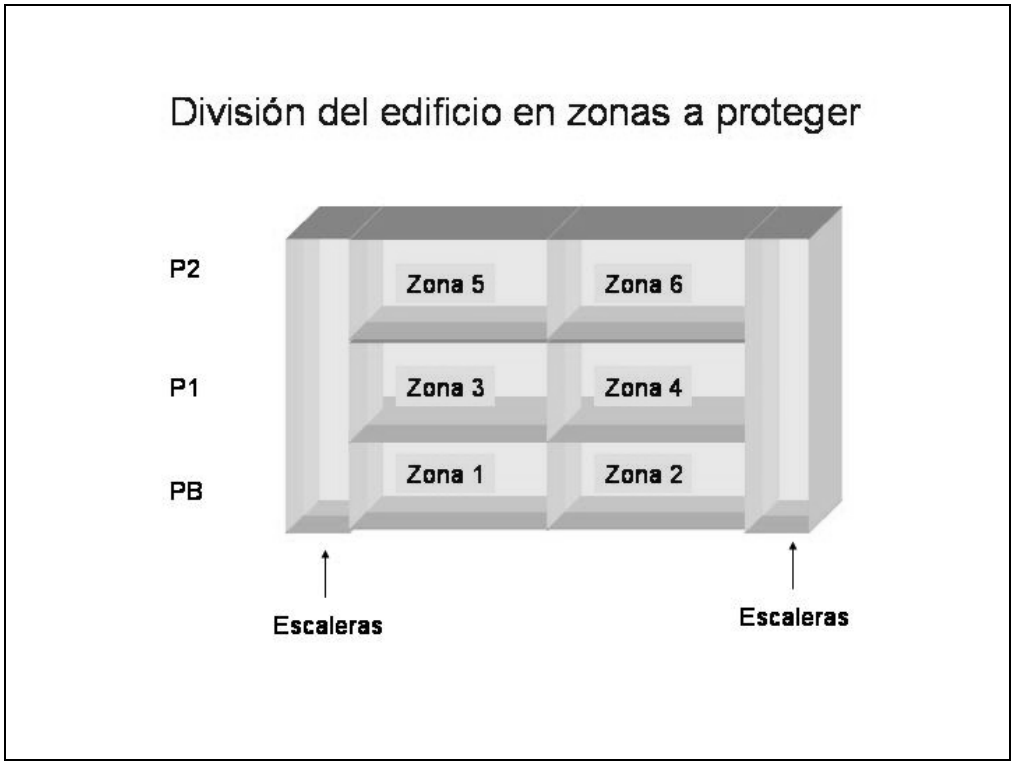


Ilustración 1. División del edificio en zonas a proteger

Sensores

Son dispositivos electrónicos que están distribuidos por todo el edificio y que, según sea el caso, estarán sensando la presencia de intrusos en el recinto, la presencia de fuego o ruptura de vidrios. Todos los sensores poseen un transmisor en la banda de 400MHz con el cual se comunican con su Maestro de Zona (MZ).

Maestro de Zona (MZ)

Dentro de cada zona de seguridad, los dispositivos que reciben los datos enviados por los sensores en la banda de 400MHz y los envían al CCGR en la banda de

2.4GHz usando los repetidores (RP) son los llamados MZ. Estos dispositivos constantemente reciben los mensajes enviados por los sensores y cuando reciben una alarma o detectan un nuevo dispositivo en su zona, envían esta información al Centro de Control y Gestión de Red (CCGR).

Repetidor (RP)

Es un dispositivo cuyo propósito, como lo indica su nombre, es el de repetir los mensajes que le son enviado para así asegurar que estos mensajes lleguen a su destino, sea un mensaje enviado por un MZ, un RP o por el CCGR.

Centro de Control y Gestión de Red (CCGR)

El CCGR es el lugar donde se concentra la información de todo lo que está sucediendo en el sistema. En el se procesan los datos que se reciben desde los sensores, MZ o RP y es aquí donde se determina si existe una situación irregular en el recinto o sí por el contrario todo está normal.

Cabe destacar que el CCGR es el único punto desde donde se puede encender o apagar dispositivos terminales como los sensores de presencia, así como hacer modificaciones a la configuración del sistema. Es en el CCGR donde se determina que mensajes se generan y envía los reportes hacia el centro de vigilancia de la facultad y otros entes como los bomberos, para así atender en cada caso la eventualidad presente el la EIE de la UCV.

Metodología usada para desarrollar el protocolo

Para el desarrollo del protocolo de comunicaciones para el sistema de seguridad de la EIE de la UCV se siguió la siguiente metodología:

- Se determinó que características debía tener el sistema de seguridad a implementar en la EIE de la UCV
- Se investigó sobre los diferentes protocolos de comunicaciones industriales y comerciales de mayor extensión
- Se investigó sobre los diferentes dispositivos y sistemas de seguridad que existen en el mercado
- Tomando en cuenta los puntos anteriores se propone una arquitectura lógica y física para el sistema de seguridad inalámbrico y se recomiendan algunos equipos
- Luego se desarrolla el protocolo para hacer posibles las comunicaciones entre los diferentes dispositivos que conformarán el sistema de seguridad en función de las características de los equipos y las características del sistema de seguridad
- Se establecen los mensajes a ser enviados por los diferentes dispositivos que conforman el sistema de seguridad y la codificación de los datos
- Con el protocolo, los mensajes y la arquitectura del sistema de seguridad se desarrolla el método para crear direcciones y rutas para poder configurar el sistema

Desarrollo del protocolo

Características del sistema de seguridad para la EIE

El sistema de seguridad que se desea implantar debe tener las siguientes características a nivel de protección:

- Detectar intrusos en las diferentes áreas del edificio.
- Controlar el acceso a ciertos espacios controlados.
- Detectar la presencia de fuego en la edificación.
- Detectar si las ventanas son violentadas

A nivel de infraestructura, el sistema debe:

- Concentrar toda la información en un solo punto de la red
- Informar de cualquier falla de comunicación en el sistema
- Informar cuando un componente de la red es violentado o su batería está baja
- Si algún componente importante de la red dejara de funcionar el sistema debe detectarlo e intentar recuperar las comunicaciones con el área afectada activando equipos de respaldo

Investigación sobre los protocolos comerciales e industriales

Para el desarrollo del protocolo de comunicaciones para el sistema de seguridad, se revisaron diferentes protocolos comerciales e industriales, entre estos están:

- Frame Relay
- Las recomendaciones 802.11 de la IEEE
- Bluetooth
- Las recomendaciones 802.15 de la IEEE
- MODBUS

Los protocolos Frame Relay, están diseñados para el intercambio de datos y dar conexión directa a Internet utilizando enlaces de circuitos virtuales. Estos protocolos están basados en el protocolo X.25, que trabaja solamente en los dos primeros niveles del modelo OSI, capa física y de enlace de datos.

El protocolo 802.11 es un estándar de protocolo de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capa física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN (Wireless Local Area Network o red de área local inalámbrica).

Por su parte, Bluetooth es una norma que define un estándar global de comunicación inalámbrica, que permite la transmisión de voz y datos entre diferentes equipos mediante un enlace por radiofrecuencia. Los principales objetivos que se pretende conseguir con esta norma son facilitar las comunicaciones entre equipos móviles y fijos, eliminar cables y conectores entre éstos, ofrecer la posibilidad de

crear pequeñas redes inalámbricas y además facilitar la sincronización de datos entre equipos personales.

El Estándar IEEE 802.15 se enfoca básicamente en el desarrollo de estándares para redes tipo PAN o redes inalámbricas de corta distancia. Al igual que Bluetooth el 802.15 permite que dispositivos inalámbricos portátiles como PCs, PDAs, teléfonos, pagers, entre otros, puedan comunicarse e ínter operar unos con otros, pero debido a que Bluetooth no puede coexistir con una red inalámbrica 802.11x, entonces la IEEE definió este estándar para permitir la interoperatibilidad de las redes inalámbricas LAN con las redes tipo PAN.

En general, los protocolos de la rama 802.x definen la tecnología de acceso en redes de área local.

MODBUS es un protocolo de comunicaciones Maestro-Esclavo, en el cual *todos* los elementos de la red están conectados físicamente a un bus y donde cada esclavo responde cuando el maestro da la orden. Este protocolo y sus variantes (MODBUS PLUS, PROFIBUS, BITBUS, etc.) son muy utilizados en la industria para la supervisión y control de equipos.

Del estudio de los protocolos se concluye que los protocolos 802.11, los 802.15, Bluetooth, Frame Relay, están orientados a comunicaciones de alto volumen de datos en redes LAN, PAN o WLAN o están orientados a ofrecer servicios para Internet; mientras que el protocolo MODBUS y sus variantes están orientados al control de equipos industriales, pero ninguno está orientado o tiene entre sus aplicaciones la protección de una edificación, por lo cual se decide tomar las cualidades, características o beneficios de algunos de los protocolos para armar parte del protocolo a ser usado en el sistema de seguridad. Este protocolo utilizará algunas fortalezas de los protocolos antes mencionados para la aplicación específica de "sistema de seguridad"

Entre los elementos que se tomarán para el desarrollo del protocolo de comunicaciones están:

- El enrutamiento de los mensajes como en el protocolo Frame Relay.
- Las funciones de lectura/escritura de registro del protocolo MODBUS.
- La concentración de las comunicaciones de los dispositivos hacia un solo elemento de red, como en los protocolos 802.11, 802.15 y Bluetooth.

Investigación sobre sensores y sistemas de seguridad

De la investigación realizada sobre los diferentes sistemas de seguridad y equipos existentes en el mercado para realizar tareas de detección y protección de ambientes, se observó que son muy variados tanto en funcionamiento como en sus características. Entre los equipos comerciales utilizados para los sistemas de seguridad se tienen:

- Sensores de presencia
- Sensores contra incendio
- Sensores de vibración o ruptura
- Sensores de apertura
- Sistemas de control de acceso

Los sensores de presencia son dispositivos que, como indica su nombre, detectan la presencia de masas en movimiento en un área específica; los sensores de presencia mas comunes son a) sensores de infrarrojo: que detectan los cambios térmicos para determinar la presencia de intrusos en un área, b) sensores de movimiento: por cambios en la posición de los objetos frente a ellos y c) sensores de presencia mixtos: que usan las tecnología de los dos sensores anteriormente descritos para detectar la presencia de intrusos en algún área.

Los sensores contra incendios son dispositivos encargados de determinar si existe fuego en un recinto; los hay de varias tecnologías, a saber: a) detectores de infrarrojo, b) detectores de gases y c) detectores mixtos.

Los sensores de vibración o ruptura, son dispositivos que se usan para detectar cuando un cristal es golpeado o cuando un objeto es movido.

Los sensores de apertura son dispositivos que detectan cuando una puerta es abierta o cerrada, normalmente estos dispositivos son del tipo magnético y cuando las partes del dispositivo son juntadas o separadas se abre o cierra un circuito, detectando así la apertura de la puerta.

Los sistemas de control de acceso son dispositivos que se usan para saber cuantas personas entran a un recinto y sus identidades, ya que para entrar a un recinto cada persona debe ingresar un código de acceso o presentar su huella dactilar para que el sistema determine si está o no autorizado a entrar y así permitir que la puerta se abra o no.

Una característica común en todos los dispositivos comerciales es que están diseñados para realizar la comunicación de su estado en forma cableada sin embargo la adaptación a una comunicación inalámbrica no presenta dificultad. Son pocos los sistemas de seguridad comerciales que están diseñados para tener comunicaciones inalámbricas y, por lo general, no todo el sistema es inalámbrico, solo algunos dispositivos que lo componen.

Arquitectura propuesta para el sistema de seguridad

De la investigación sobre equipos y de las características de seguridad que se desea para el sistema, se propone la siguiente estructura:

- Se propone una arquitectura en la que se divide el edificio en zonas a ser protegidas.
- Dentro de cada zona estarán ubicados los sensores y un dispositivo en el cual se concentrarán los datos enviados por estos.
- Por la estructura física del edificio se plantea la posibilidad de utilizar elementos repetidores de la información que está siendo sensada en cada zona y que se está concentrando en los elementos centrales de cada zona (MZ).
- Tener dos niveles de comunicación, ubicadas en dos bandas de frecuencias distintas ISM (bandas que no requieren licencias), una banda en donde se comunican los sensores hacia el elemento central en cada zona, llamados MZ y otra banda para las comunicaciones entre los MZ, RP y el CCGR.
- Para la banda en la que se comunicarán los sensores se propone la banda de 400MHz (desde 300MHz hasta 500MHz), en la cual existen transmisores y receptores que trabajan el las frecuencias fijas de: 315MHz, 418MHz y 433MHz
- Para la banda en la que se comunicarán los MZ, los RP y el CCGR se propone la banda de 2.4GHz (desde 2.4GHz hasta 2.525GHz), la cual consta de 125 canales disponibles, cada uno con un ancho de banda de 1MHz
- La comunicación se hará de los sensores hacia los MZ en la banda de 400MHz y estos enviarán la información recibida desde los sensores hacia el CCGR a través de los RP en la banda de 2.4GHz

Equipos propuestos para realizar las comunicaciones

- Para la banda de 400MHz se recomienda el uso de los equipos de transmisión y recepción TLP434A y RLP434A respectivamente de Laipac Technology, Inc., para datos técnicos ver anexo 1

- Para la banda de 2.4GHz se recomienda el uso del transceiver (transceptores) TRF-24G de Laipac Tecnology Inc., datos técnicos ver anexo 2

Protocolos del sistema de seguridad EIE UCV 2006 V.0

Este protocolo para el sistema de seguridad inalámbrico es un protocolo ***mixto***, el cual, por un lado es un protocolo propietario en donde se establecen los formatos de los mensajes y las secuencias de estos, para todos los mensajes en el sistema, pero cuando los mensajes son de *configuración* o de *petición de reporte de estado* a los diferentes componentes del sistema de seguridad, "la estructura" de datos dentro del mensaje usan secuencias y funciones que son del protocolo MODBUS, ya que existen funciones definidas en este protocolo que permiten realizar estas acciones

El protocolo de comunicaciones para el sistema de seguridad se desglosa en otros protocolos específicos que se ejecutan en cada dispositivo que conforma el sistema de seguridad, teniéndose al final el siguiente conjunto de protocolos:

- Protocolos para el Centro de Control y Gestión de Red.
- Protocolos para los Maestro de zona.
- Protocolos para los Repetidores.
- Protocolos para los sensores.

Protocolos del CCGR

En el Centro de Control y Gestión de Red se ejecutan protocolos, que según sea el caso, tendrán secuencias específicas. Los tipos de secuencia son:

- Configuración del sistema.
- Sondeo o supervisión del sistema.
- Manejo de alarmas y reportes.

En la ilustración 2 se muestra como en un momento dado pudiera darse el flujo de datos en el sistema en la banda de 2.4GHz.

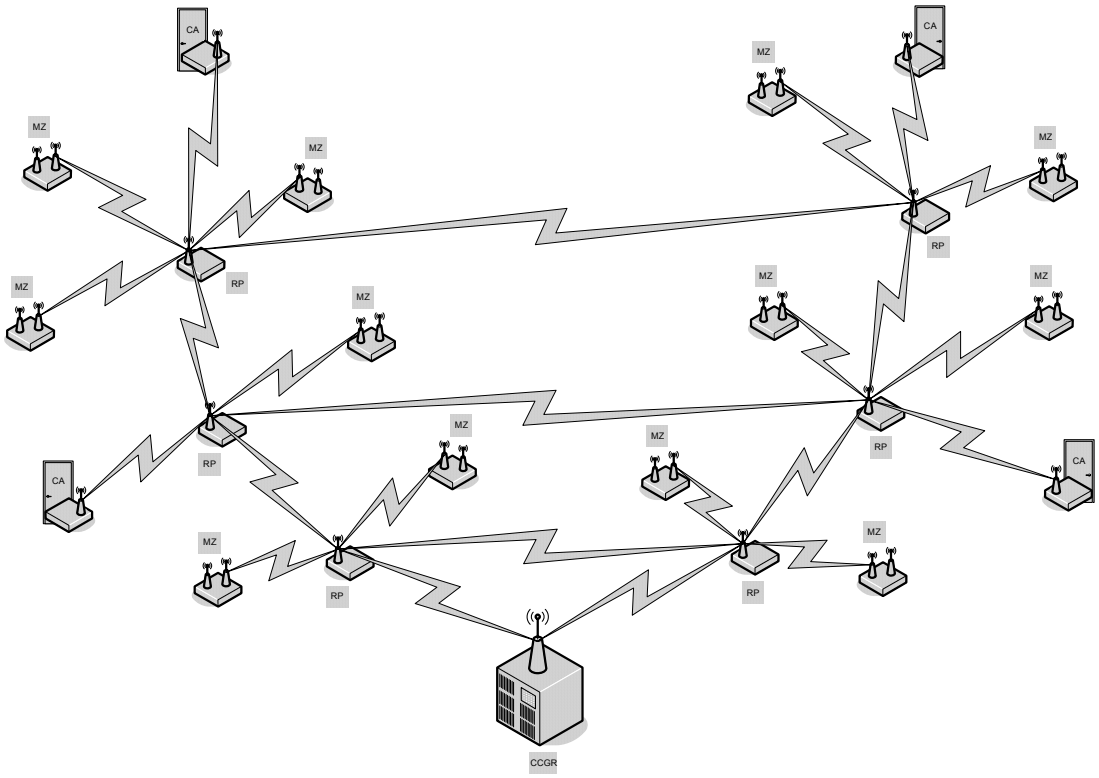


Ilustración 2. Flujo de información dentro del sistema de seguridad en un momento cualquiera

Primeramente el CCGR, así como todos los dispositivos que se comunican en la banda de 2.4GHz, tienen como parte de su protocolo la instrucción de enviar una confirmación de recibido al dispositivo emisor del mensaje.

Por otro lado, todos los dispositivos en la banda de 2.4GHz manejan dos canales para comunicarse, uno para control y supervisión del sistema y el otro, exclusivamente, para el manejo de las alarmas.

Protocolo de configuración del sistema

Para configurar el sistema se envían mensajes individualmente a cada dispositivo y la secuencia de configuración puede verse como una configuración por niveles o anillos, la secuencia de configuración se muestra en la ilustración 3.

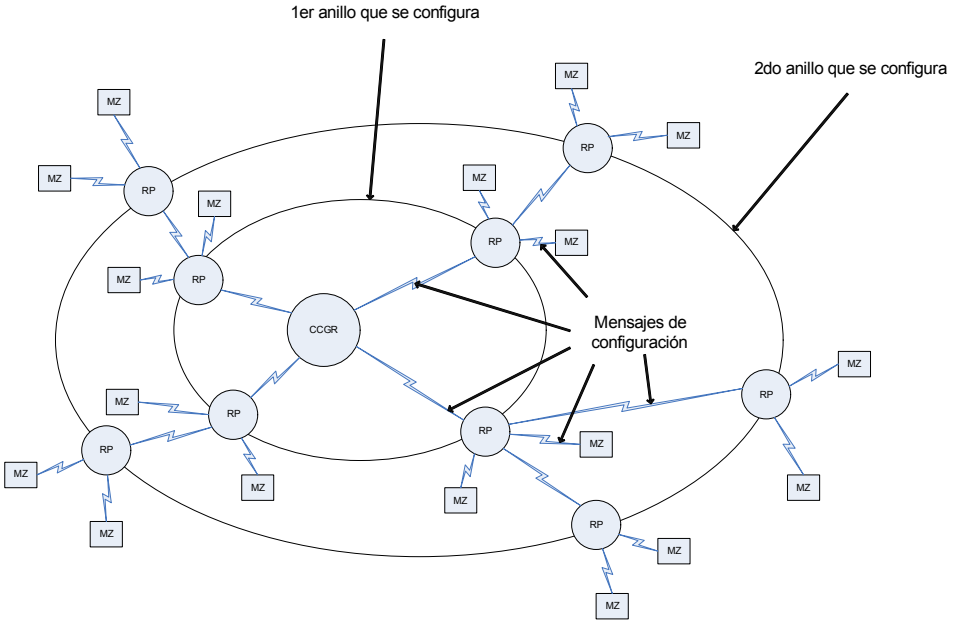


Ilustración 3. Secuencia anular para el cambio en la configuración del sistema

Esta secuencia se debe a que cuando se configura el sistema, los RP mas cercanos al CCGR se configuran primero puesto que éstos deben conocer qué dispositivos se encuentran en su entorno para así poder realizar su función de repetir, de esta manera se configuran primero los RP en cada anillo y, posteriormente, se configuran los MZ.

Es importante tomar en cuenta que cada vez que se va a realizar un cambio en la configuración del sistema, el CCGR realiza una solicitud de reporte de estado del sistema para verificar que todo el sistema está trabajando correctamente, luego de realizado este chequeo se pueden hacer los cambios y, concluidos los cambios, se

realiza nuevamente un chequeo al sistema para así corroborar que no hay fallas o, por el contrario, para detectar las fallas debidas a la nueva configuración y corregirlos haciendo los cambios pertinentes. Esta configuración remota se realizará en el caso de haber cambiado algún equipo repetidor o maestro de zona.

Protocolo para petición del reporte de estado a los MZ y RP

La forma en que se platea la supervisión o monitoreo de los elementos que componen el sistema de seguridad es a través de la petición del reporte de estado a los MZ y a los RP, de esta manera el CCGR puede saber si todos los sensores, MZ y RP están activos y cuando fue la última vez que cada sensor se reportó con el MZ. El reporte de estado se solicita a cada componente en la banda 2.4GHz de forma individual, comenzando por los RP y sus respaldos y luego los MZ y sus respaldos.

Si no respondiera un RP o un MZ el protocolo establece que el CCGR activará el respaldo del dispositivo en cuestión y volverá a realizar el monitoreo del sistema, generando un reporte indicando qué zona(s) debe(n) ser atendida(s).

En el caso de que no respondiera un MZ y su respaldo, se generará una alarma indicando una falla en el sistema y un reporte indicando qué zona(s) debe(n) ser atendida(s) con urgencia.

En el caso de ser un RP y su respaldo, se generará una alarma indicando falla general del sistema y en el reporte se indicarán todas las zonas afectadas.

Protocolo para cambio de canal del sistema

Para aumentar la seguridad del sistema, se plantea el cambio de frecuencia de los canales de control y de alarma, con cierta regularidad.

A partir de un programa que se ejecuta en el CCGR, el cual calcula la frecuencia del nuevo canal y el tiempo en que se hará el cambio de canal, y llegada la hora, el CCGR realizará una solicitud de reporte de estado del sistema, si el reporte indica que el sistema está funcionando sin problemas, entonces se procederá al cambio de canal.

Para realizar el cambio de canal, el CCGR enviará mensajes a cada MZ en el anillo más alejado indicándole que se cambie de canal, cuando todos los MZ en ese anillo hayan informado que se cambiarán de canal, entonces se le indica a los RP que se cambien de canal, cambiándose luego el CCGR al nuevo canal.

Concluido el cambio de canal, se realiza otra petición de reporte de estado del sistema para verificar que todos los RP y MZ se cambiaron al nuevo canal y están trabajando correctamente.

En la ilustración 4 se muestra la secuencia por anillos del cambio de canal.

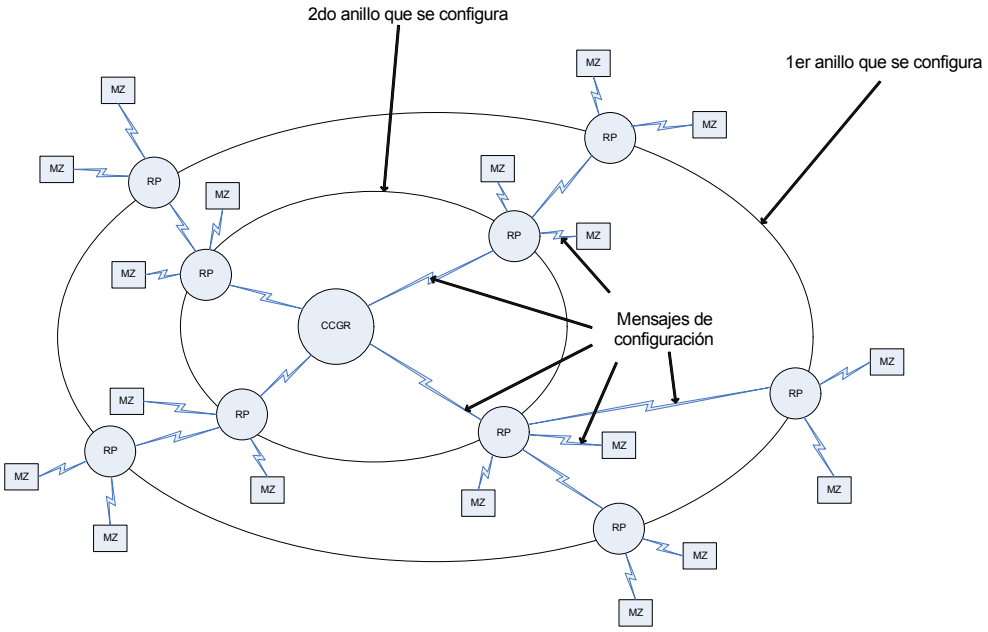


Ilustración 4. Secuencia anular para el cambio de canal de control del sistema

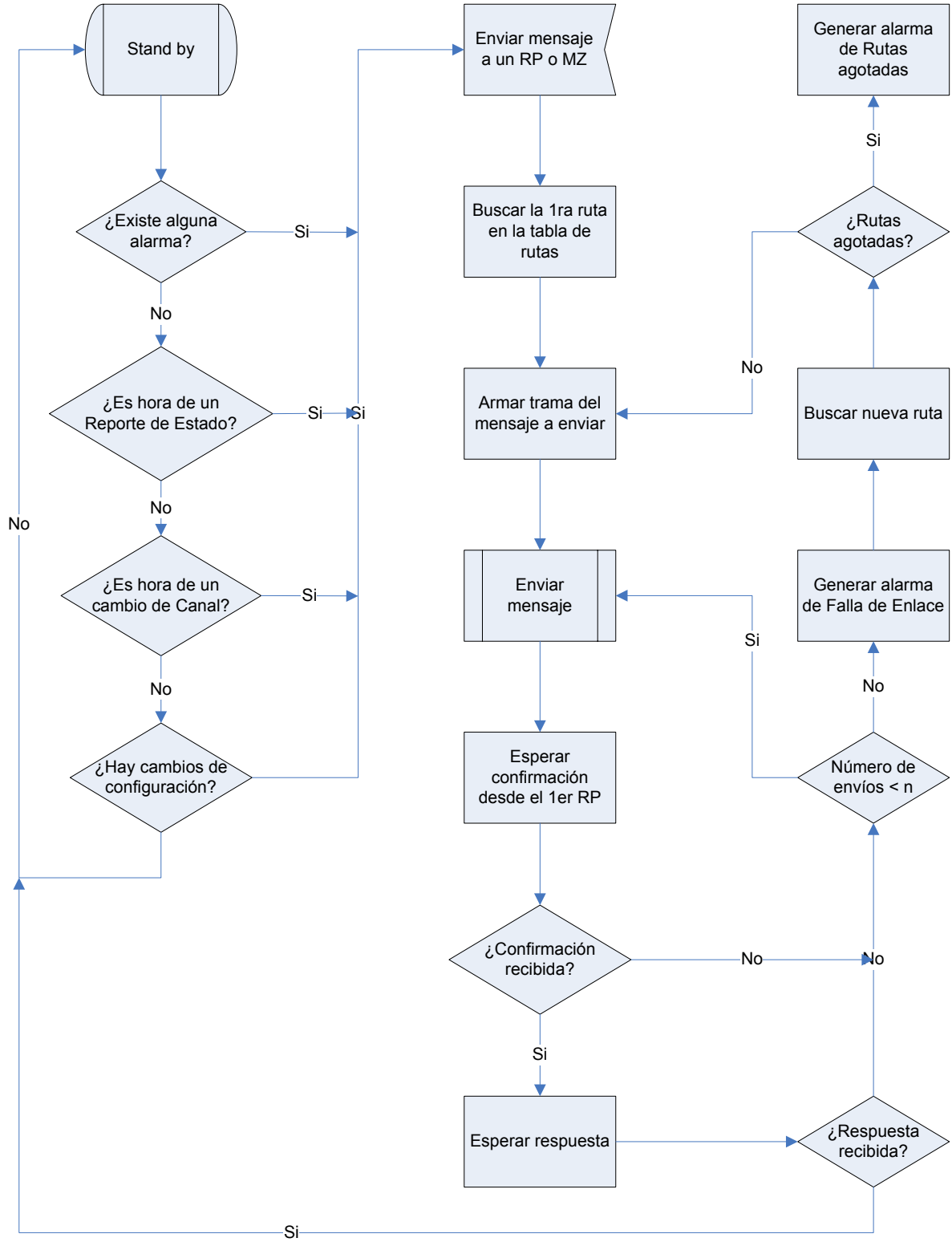
Protocolo para el manejo de alarmas

Debido a que en el recinto puede haber insectos y roedores que pueden en un momento dado activar un sensor de presencia y hacer que el sistema envíe mensajes de alarma, se implementa en el CCGR *tablas de secuencias de alarmas.* Las tablas de secuencias de alarmas son listas de alarmas que se deben seguir en cierto orden y que le ayudan al CCGR a determinar si la alarma recibida es o no una alarma real.

Cuando el CCGR recibe una alarma, verifica en su tabla de secuencias y según el tipo de alarma y la secuencia indicada en la tabla el CCGR esperará o no hasta recibir otra alarma para llevar a cabo acciones como la de llamar a la vigilancia o a los bomberos.

En la ilustración 5 se muestra un diagrama simplificado del protocolo del CCGR, para mas detalles ver anexo 3.

Ilustración 5. Diagrama de flujo simplificado del Protocolo del CCGR



Protocolos de los RP

Protocolo para transferencia de datos y alarmas

Cada RP, después de recibir un mensaje y confirmar al dispositivo que le envió el mensaje, que lo recibió; busca en su tabla de rutas la dirección del dispositivo al cual debe enviar el mensaje para que éste pueda llegar a su destino; luego el RP queda en espera, por cierto tiempo, hasta recibir el mensaje de recibido por parte del dispositivo al que le envió el mensaje, de no recibirla, envía el mensaje las veces que se haya programado o hasta que se reciba la confirmación. Si no se recibiera respuesta, el RP busca en su tabla de rutas la siguiente dirección a donde debe enviar el mensaje y se repite el proceso.

Si el mensaje proviene del CCGR y un RP ó MZ al que se le repite el mensaje no respondiera, el RP que está repitiendo el mensaje, envía otro mensaje al CCGR indicando qué dispositivo no respondió.

Protocolo para configuración y cambio de canal del RP

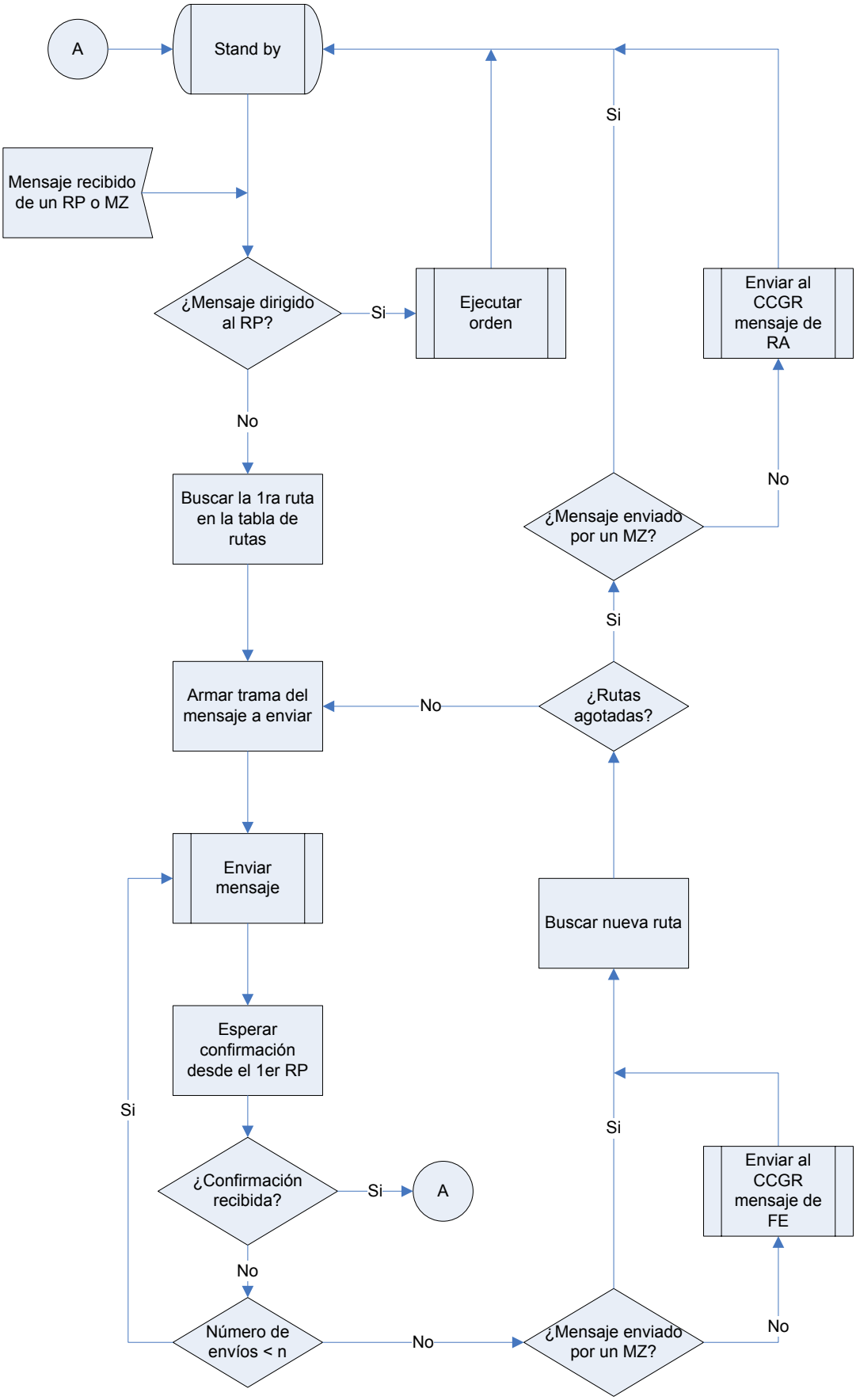
Cuando el RP recibe un mensaje de cambio de canal o de configuración, envía la confirmación de que recibió el mensaje, toma los datos y envía un mensaje al CCGR indicando que va a comenzar a realizar los cambios. Una vez efectuado los cambios el RP quedará nuevamente en espera.

Reporte de estado del RP

Cuando el RP recibe un mensaje desde el CCGR para que indique cual es su estado, el RP lee su nivel de batería y envía al CCGR esta información, así el CCGR no sólo sabe que el RP está funcionando, sino también cual es su nivel de batería.

En la ilustración 6 se muestra un diagrama simplificado del protocolo del RP, para mas detalles ver anexo 4.

Ilustración 6. Diagrama de flujo simplificado del Protocolo del RP



Protocolos de los MZ

Protocolo para configuración y cambio de canal

Cuando un MZ recibe un mensaje para realizar cambio de canal o de configuración, envía la confirmación de que recibió el mensaje, toma los datos y envía un mensaje al CCGR indicando que va a comenzar a realizar los cambios. Luego de hechos los cambios, el MZ quedará en espera.

Petición de reporte de estado

Cuando un MZ recibe, desde el CCGR, la petición de reporte de estado, el MZ responde enviando su nivel de batería y la tabla de los dispositivos asignados a él que no se reportaron en un tiempo determinado.

Protocolo para reporte de dispositivo nuevo detectado

Cada vez que un MZ recibe un mensaje desde un sensor, verifica en la trama si el dispositivo está asignado a él, de no estarlo se descarta la trama, en caso contrario, procede a revisar en su tabla de dispositivos habilitados y de no encontrarse, se envía una trama al CCGR por el canal de alarmas indicando que un nuevo sensor fue localizado, en este mensaje se incluye el identificador del sensor y si el mensaje enviado por el sensor es una alarma, entonces se envía el tipo de alarma que está enviando el sensor en cuestión.

Protocolo para el manejo de alarmas

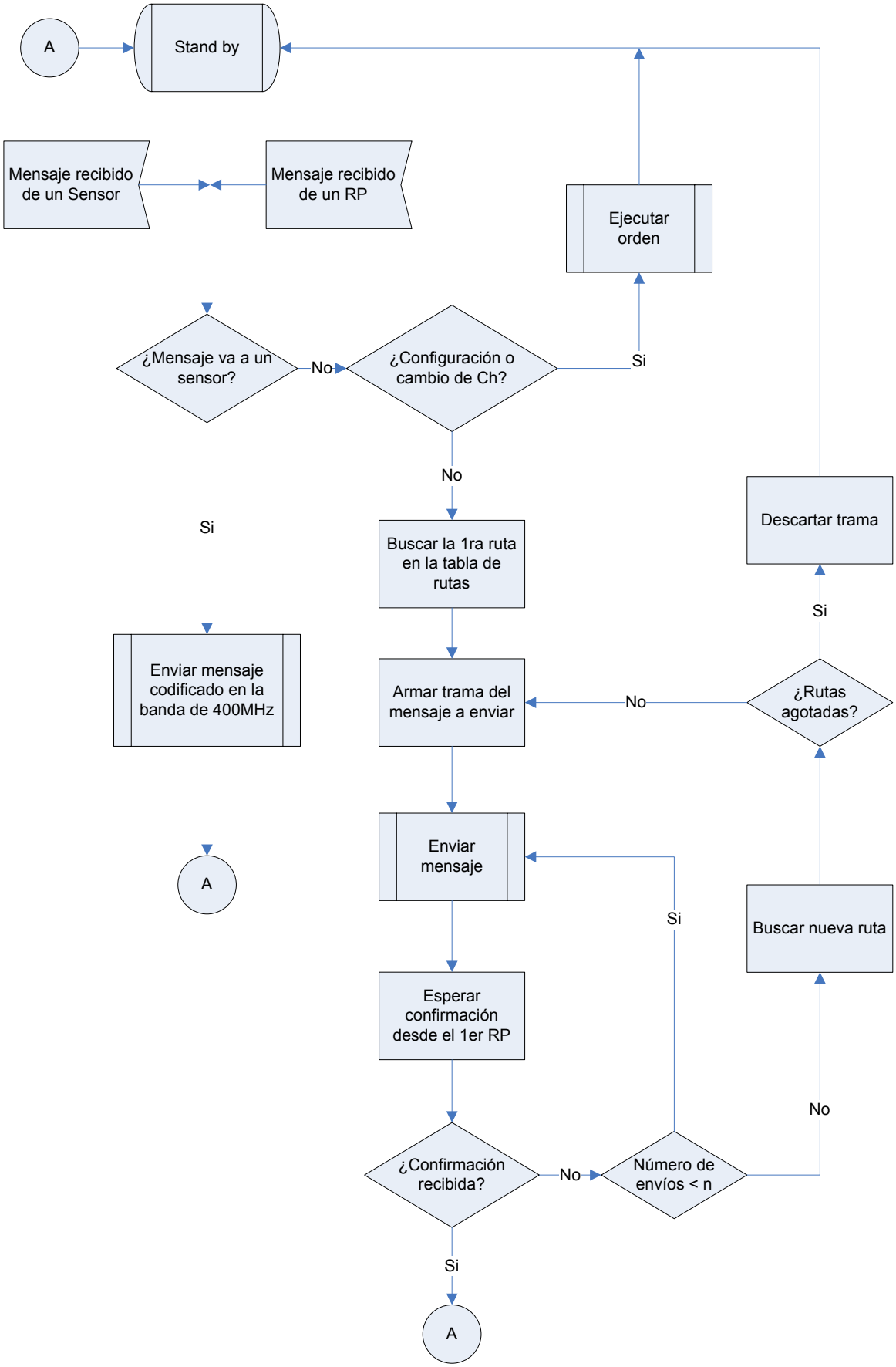
Cada vez que un MZ recibe un mensaje que proviene de un sensor, el MZ verificará si el mensaje proviene de un elemento que le fue asignado, de no serlo desechará el mensaje, si se tratará de un sensor que sí está en su lista de dispositivos habilitados, entonces toma el identificador del sensor y el código de la alarma que está enviando y enviará un mensaje al CCGR por el canal de alarma, en este mensaje va el identificador del sensor, la zona a la que está asignado y el tipo de alarma y si se tratara de una alarma de incendio el MZ activará una sirena para informar al público que hay fuego en la zona.

Protocolo para el manejo de sensores o actuadores

Cuando el MZ recibe un mensaje para apagar o encender un sensor u otro dispositivo del sistema, el MZ revisa si el dispositivo en cuestión está asignado a él, de no estarlo informa al CCGR que el dispositivo no existe en su lista y desecha el mensaje; de estar en su lista, el MZ envía un mensaje en la banda de 400MHz indicando al dispositivo qué acción debe realizar.

En la ilustración 7 se muestra un diagrama simplificado del protocolo del MZ, para mas detalles ver anexo 5.

Ilustración 7. Diagrama de flujo simplificado del Protocolo del MZ



Protocolo de los sensores

En la banda de 400MHz todos los sensores están programados para realizar reportes periódicos indicando que están presentes y que todo está normal; de producirse una irregularidad los sensores envían esta información al MZ al cual están asignados.

En ésta banda de 400MHz sólo los sensores de presencia y los actuadores, como las sirenas contra incendios, poseen receptores en la banda de 400MHz, el resto de los sensores están siempre activos. Por otro lado, los sensores al intentar comunicar su estado o una irregularidad que se esté produciendo en el recinto, no pueden saber sí algún otro dispositivo está transmitiendo, lo cual implica que habrá momentos en que dos o más sensores en la banda de 400MHz que estén asignados a un mismo MZ estarán transmitiendo simultáneamente, esto hará que el MZ no reciba el mensaje de ninguno de los sensores que está transmitiendo. Para resolver esta situación se programa a los sensores para que cada vez que suceda una eventualidad transmitan el suceso cinco veces al MZ, pero los tiempos entre las cinco tramas es aleatorio y siempre mayor que el tiempo de transmisión de una trama de la banda de 400MHz, de forma que el MZ siempre podrá recibir al menos una de las tramas que está enviando el sensor.

Pruebas al sistema de seguridad EIE UCV 2006 V.0

Para comprobar el correcto funcionamiento del sistema de seguridad, tanto equipos como protocolo, se deben realizar las siguientes acciones y pruebas al sistema:

- Cargar el protocolo a los dispositivos.
- Instalar los dispositivos.
- Realizar pruebas de transmisión de datos
- Realizar pruebas de transmisión de alarmas.

Pruebas de transmisión de datos

Las pruebas de transmisión de datos consisten en enviar solicitudes de reporte de estado desde el CCGR y verificar que todos los dispositivos MZ y RP responden ante dicha solicitud. Con esta prueba se verifica el correcto funcionamiento del sistema en el canal de control.

Pruebas de transmisión de alarmas

Las pruebas de transmisión de alarmas consisten en generar alarmas dentro de cada zona donde se están realizando las pruebas y verificar que fueron detectadas en el CCGR. Con esta prueba se verifica el correcto funcionamiento del sistema en el canal de alarmas.

Realizadas estas pruebas se puede asegurar que el sistema estará funcionando correctamente.

CONCLUSIONES

De las pruebas realizadas al protocolo y a los equipos desarrollados para el sistema de seguridad inalámbrico se tienen las siguientes conclusiones:

1. El protocolo desarrollado cumplió con todos los necesidades y requerimientos del sistema
2. Debido al algoritmo de reenvío de tramas, se asegura que dos dispositivos de la banda de 2.4GHz que estén en funcionamiento normal y que traten de comunicarse, lo podrán hacer sin problemas.
3. Debido al número de chequeos que se realizan a las tramas durante la transmisión de los mensajes, éstos llegan a su destino sin errores.
4. Debido al algoritmo de reenvío de tramas que se ejecuta en los dispositivos sensores, se asegura que los mensajes enviados por un sensor siempre serán recibidos por su respectivo Maestro de Zona.
5. Debido a la codificación que se lleva a cabo en los dispositivos sensores se asegura que los datos recibidos por los Maestros de Zona son datos válidos y libres de errores.
6. Debido a las formas de codificación que se usan tanto en la banda de 2.4GHz como en la de 400MHz se asegura que todos los mensajes son único en la red.
7. Adicionalmente a todas las cualidades mencionadas y debido a la utilización de algunas funciones MODBUS dentro de las tramas en el sistema, la red creada puede utilizarse para el control de otros equipos tales como luminarias, aires acondicionados, etc.

RECOMENDACIONES

1. Para la configuración del sistema y reducir los errores en las tablas de rutas a ser grabadas en todos los dispositivos que trabajan en la banda de 2.4GHz se recomienda el uso del programa SSEIEUCV2006V3 desarrollado para tal fin durante el proyecto.
2. En la modalidad de seguridad del sistema se recomienda modificar y optimizar la estructura de datos usadas en las tramas, para que ocupen un menor número de bytes, logrando con esto dos (2) cosas:

    - Aumentar el número de dispositivos que operan en la banda de 2.4GHz
    - Disminuir la cantidad de tramas que hay que enviar a un dispositivo cuando se desee reconfigurarlo completamente

3. Para el momento en que se hizo la selección de los equipos se escogió el tranceptores TRF-24G de Laipac Tecnology Inc. basado en el circuito integrado nRF2401 de Nordic Semiconductor. Actualmente, y gracias a los desarrollos en esta tecnología existen en el mercado varios circuitos integrados (como el nRF24Z1, el nRF24E1 entre otros) que poseen una mayor velocidad de transmisión y un menor consumo de energía, y además son compatibles con todas las aplicaciones de los tranceptores que se usaron en este proyecto.

BIBLIOGRAFÍA

Libros

- TANENBAUM, Andrew. Redes de ordenadores. 2da. Edición. México: Prentice-Hall, 1991

Tesis

- Ortega, Camilo. Diseño de un sistema de seguridad inalámbrico para uso en residencias unifamiliares / Ortega, Camilo (Tesis).-- Caracas: Universidad Central de Venezuela, 2003
- Zamorano, Roberto. Sistema de seguridad inalámbrico, programable con auto-chequeo. / Zamorano, Roberto (Tesis).—Caracas: Universidad Central de Venezuela, 2003.

Referencias digitales

- http://www.sc.ehu.es/acwamurc/JCRA_Protocolo.pdf
- http://iio.ens.uabc.mx/~jmilanez/escolar/redes/03020000.html#capas
- http://www.monografias.com/trabajos14/datos-redes/datos-redes.shtml#TOPO
- http://www.unav.es/cti/manuales/Redes_Internet/
- http://es.wikipedia.org/wiki/Protocolos_de_red
- http://es.wikipedia.org/wiki/Modelo_de_interconexi%C3%B3n_de_sistemas_abiertos
- http://www.google.co.ve/search?hl=es&lr=&oi=defmore&defl=es&q=define:Protocolo
- http://www.servitel.es/atv/AYU/INTERNET/DICCGRIO/diCCGRio.htm
- http://www.rediris.es/moviris/tecnologias/
- http://www.redlibre.net/modules.php?name=Encyclopedia&op=content&tid=162
- http://www.gammainternet.com/tecnologia/wireless/normas.html
- http://html.rincondelvago.com/protocolos-de-comunicaciones.html
- http://www.grulic.org.ar/eventos/demoday6/material/filminas/wlan_2.pdf.gz

GLOSARIO

ASCCI	American Standard Code for Information Interchange
BIT BUS	Protocolo industrial basado en MODBUS
CCGR	Centro de Control y Gestión de Red
EBCDIC	Extended Binary Coded Decimal Interchange Code
HTTP	HiperText Transfer Protocol
ISM	Industrial Scientics and Medical
LAN	Local Area Network
LLC	Logical Link Control
MAC	Media Access Control
MODBUS	Protocolo de comunicaciones para equipos de control automatizado
MODBUS PLUS	Protocolo industrial basado en MODBUS
MZ	Maestro de Zona
NZR	Codificación de línea sin retorno a cero
OSI	Open System Interconection
PAN	Personal Area Network
PCs	Personal Computers
PDAs	Personal Digital Asistants
PROFIBUS	Process Field Bus
RF	Radio Frecuencia
RP	Repetidor
WLAN	Wireless Local Area Network

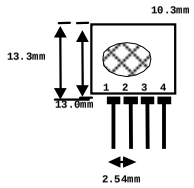
ANEXOS

ANEXO 1

TLP434A & RLP434A **RF** ASK Hybrid Modules for Radio Control (New Version)

TLP434A Ultra Small Transmitter

Easy-Link Wireless



pin 1 : GND
pin 2 : Data In
pin 3 : Vcc
pin 4 : Antenna (RF output)

Frequency 315, 418 and 433.92 Mhz

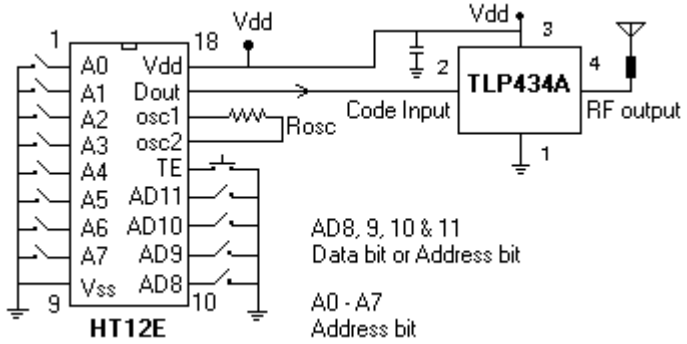
Modulation : ASK
Operation Voltage : 2 - 12 VDC

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
Vcc	Operating supply voltage		2.0	-	12.0	V
Icc 1	Peak Current (2V)		-	-	1.64	mA
Icc 2	Peak Current (12V)		-	-	19.4	mA
Vh	Input High Voltage	Idata= 100uA (High)	Vcc-0.5	Vcc	Vcc+0.5	V
Vl	Input Low Voltage	Idata= 0 uA (Low)	-	-	0.3	V
FO	Absolute Frequency	315Mhz module	314.8	315	315.2	MHz
PO	RF Output Power- 50ohm	Vcc = 9V-12V	-	16	-	dBm
		Vcc = 5V-6V	-	14	-	dBm
DR	Data Rate	External Encoding	512	4.8K	200K	bps

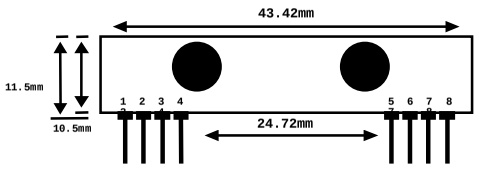
Notes : (Case Temperature = 25°C +- 2°C , Test Load Impedance = 50 ohm)

Application Circuit :

Typical Key-chain Transmitter using HT12E-18DIP, a Binary 12 bit Encoder from Holtek Semiconductor Inc.



RLP434A SAW Based Receiver



pin 1 : Gnd
pin 2 : Digital Data Output
pin 3 : Linear Output /Test
pin 4 : Vcc
pin 5 : Vcc
pin 6 : Gnd
pin 7 : Gnd
pin 8 : Antenna

Frequency 315, 418 and 433.92 Mhz

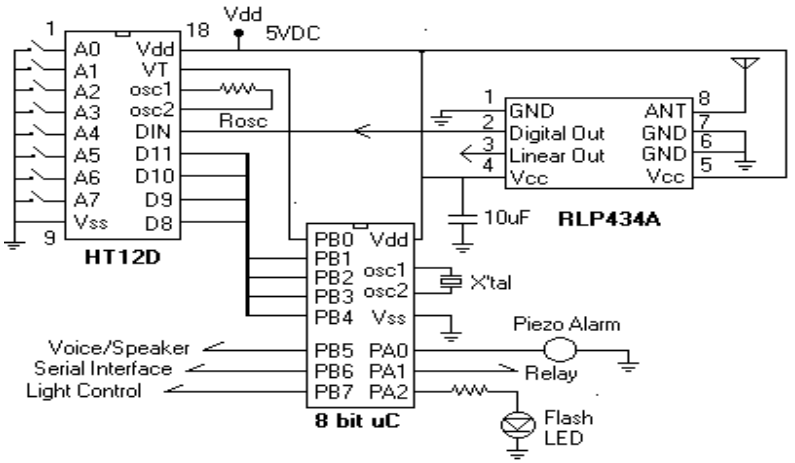
Modulation : ASK
Supply Voltage : 3.3 - 6.0 VDC
Output : Digital & Linear

Symbol	Parameter	Conditions	Min	Typ	Max	
Vcc	Operating supply voltage		3.3	5.0V	6.0	V
Itot	Operating Current		-	4.5		mA
Vdata	Data Out	Idata = +200 uA (High)	Vcc-0.5	-	Vcc	V
		Idata = -10 uA (Low)	-	-	0.3	V

Electrical Characteristics					
Characteristics	SYM	Min	Typ	Max	Unit
Operation Radio Frequency	FC	315, 418 and 433.92			MHz
Sensitivity	Pref		-110		dBm
Channel Width			+-500		Khz
Noise Equivalent BW			4		Khz
Receiver Turn On Time			5		ms
Operation Temperature	Top	-20	-	80	C
Baseboard Data Rate			4.8		KHz

Application Circuit :

Typical RF Receiver using HT12D-18DIP, a Binary 12 bit Decoder with 8 bit uC HT48RXX from Holtek Semiconductor Inc.



Laipac Technology, Inc.
105 West Beaver Creek Rd. Unit 207 Richmond Hill Ontario L4B 1C6 Canada
Tel: (905)762-1228 Fax: (905)763-1737 e-mail: info@laipac.com

LAIPAC TECH

ANEXO 2

Single chip 2.4 GHz Transceiver **nRF2401**

FEATURES

- True single chip GFSK transceiver in a small 24-pin package (QFN24 5x5mm)
- Data rate 0 to1Mbps
- Only 2 external components
- Multi channel operation
  - 125 channels
  - Channel switching time <200µs.
  - Support frequency hopping
- Data slicer / clock recovery of data
- Address and CRC computation
- DuoCeiver™ for simultaneous dual receiver topology
- ShockBurst™ mode for ultra-low power operation and relaxed MCU performance
- Power supply range: 1.9 to 3.6 V
- Low supply current (TX), typical 10.5mA peak @ -5dBm output power
- Low supply current (RX), typical 18mA peak in receive mode
- 100 % RF tested
- No need for external SAW filter
- World wide use

APPLICATIONS

- Wireless mouse, keyboard, joystick
- Keyless entry
- Wireless data communication
- Alarm and security systems
- Home automation
- Surveillance
- Automotive

- Telemetry
- Intelligent sports equipment
- Industrial sensors
- Toys

GENERAL DESCRIPTION

nRF2401 is a single-chip radio transceiver for the world wide 2.4 - 2.5 GHz ISM band. The transceiver consists of a fully integrated frequency synthesizer, a power amplifier, a crystal oscillator and a modulator. Output power and frequency channels are easily programmable by use of the 3-wire serial interface. Current consumption is very low, only 10.5mA at an output power of -5dBm and 18mA in receive mode. Built-in Power Down modes makes power saving easily realizable.

QUICK REFERENCE DATA

Parameter	Value	Unit
Minimum supply voltage	1.9	V
Maximum output power	0	dBm
Maximum data rate	1000	kbps
Supply current in transmit @ -5dBm output power	10.5	mA
Supply current in receive mode	18	mA
Temperature range	-40 to +85	°C
Sensitivity	-90	dBm
Supply current in Power Down mode	400	nA

Table 1 nRF2401 quick reference data

MODES OF OPERATION

Overview

The nRF2401 can be set in the following main modes depending on three control pins:

Mode	PWR_UP	CE	CS
Active (RX/TX)	1	1	0
Configuration	1	0	1
Stand by	1	0	0
Power down	0	X	X

Table 6 nRF2401 main modes

For a complete overview of the nRF2401 I/O pins in the different modes please refer to Table 8.

Active modes

The nRF2401 has two active (RX/TX) modes:

- ShockBurst™
- Direct Mode

The device functionality in these modes is decided by the content of a configuration word. This configuration word is presented in configuration section.

ShockBurst™

The ShockBurst™ technology uses on-chip FIFO to clock in data at a low data rate and transmit at a very high rate thus enabling extremely power reduction.
When operating the nRF2401 in ShockBurst™, you gain access to the high data rates (1 Mbps) offered by the 2.4 GHz band without the need of a costly, high-speed micro controller (MCU) for data processing.
By putting all high speed signal processing related to RF protocol on-chip, the nRF2401 offers the following benefits:

- Highly reduced current consumption
- Lower system cost (facilitates use of less expensive micro controller)
- Greatly reduced risk of 'on-air' collisions due to short transmission time

The nRF2401 can be programmed using a simple 3-wire interface where the data rate is decided by the speed of the micro controller.
By allowing the digital part of the application to run at low speed while maximizing the data rate on the RF link, the nRF ShockBurst™ mode reduces the average current consumption in applications considerably.

ShockBurst™ principle

When the nRF2401 is configured in ShockBurst™, TX or RX operation is conducted in the following way (10 kbps for the example only).

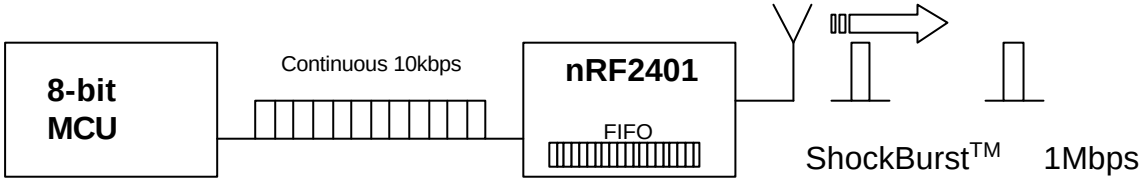


Figure 5 Clocking in data with MCU and sending with ShockBurst™ technology

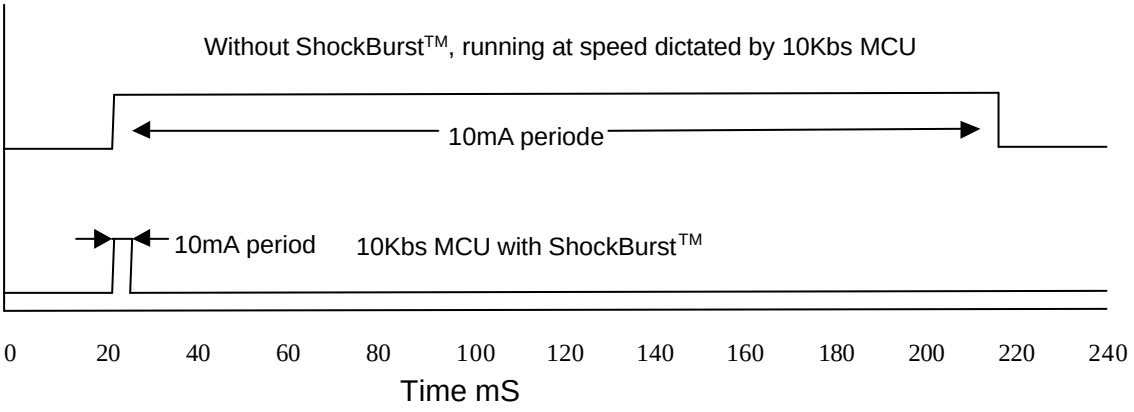


Figure 6 Current consumption with & without ShockBurst™ technology

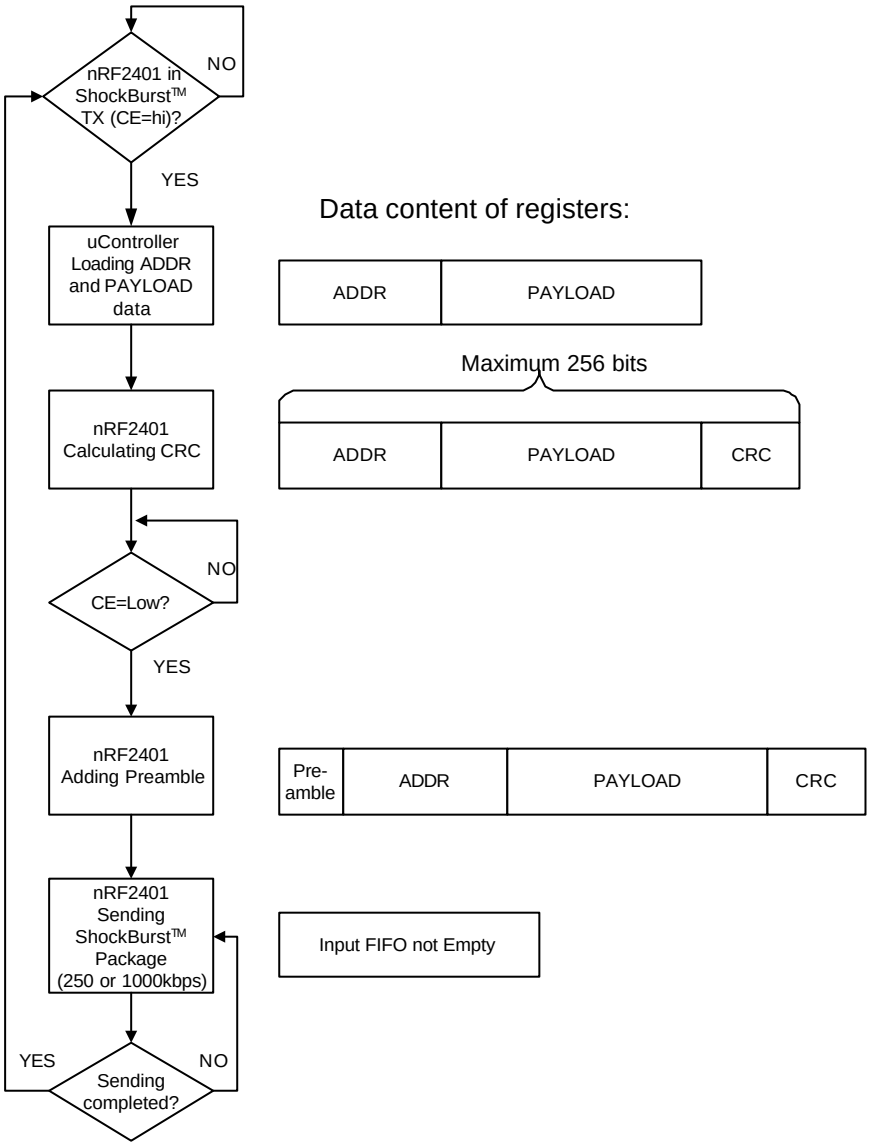


Figure 7 Flow Chart ShockBurst™ Transmit of nRF2401

nRF2401 ShockBurst™ Transmit:

MCU interface pins: CE, CLK1, DATA

1. When the application MCU has data to send, set CE high. This activates nRF2401 on-board data processing.
2. The address of the receiving node (RX address) and payload data is clocked into the nRF2401. The application protocol or MCU sets the speed <1Mbps (ex: 10kbps).
3. MCU sets CE low, this activates a nRF2401 ShockBurst™ transmission.
4. nRF2401 ShockBurst™:
   - RF front end is powered up
   - RF package is completed (preamble added, CRC calculated)
   - Data is transmitted at high speed (250 kbps or 1 Mbps configured by user).
   - nRF2401 return to stand-by when finished

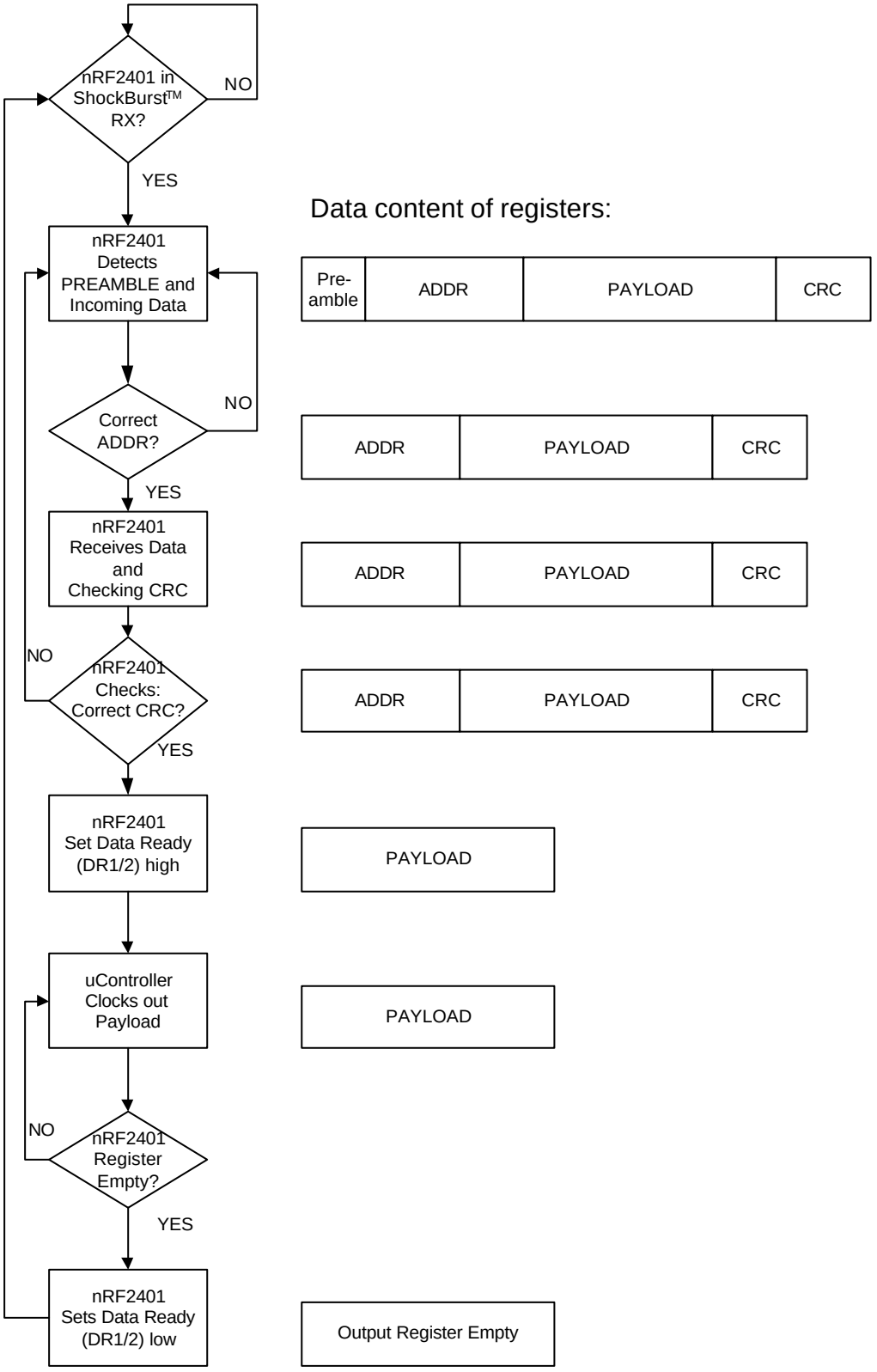


Figure 8 Flow Chart ShockBurst™ Receive of nRF2401

nRF2401 ShockBurst™ Receive:

MCU interface pins: CE, DR1, CLK1 and DATA (one RX channel receive)

1. Correct address and size of payload of incoming RF packages are set when nRF2401 is configured to ShockBurst™ RX.
2. To activate RX, set CE high.
3. After 200 µs settling, nRF2401 is monitoring the air for incoming communication.
4. When a valid package has been received (correct address and CRC found), nRF2401 removes the preamble, address and CRC bits.
5. nRF2401 then notifies (interrupts) the MCU by setting the DR1 pin high.
6. MCU may (or may not) set the CE low to disable the RF front end (low current mode).
7. The MCU will clock out just the payload data at a suitable rate (ex. 10 kbps).
8. When all payload data is retrieved nRF2401 sets DR1 low again, and is ready for new incoming data package if CE is kept high during data download. If the CE was set low, a new start up sequence can begin, see Figure 17.

Direct Mode

In direct mode the nRF2401 works like a traditional RF device. Data must be at 1Mbps ±200ppm, or 250kbps ±200ppm at low data rate setting, for the receiver to detect the signals.

Direct Mode Transmit:

MCU interface pins: CE, DATA

1. When application MCU has data to send, set CE high
2. The nRF2401 RF front end is now immediately activated, and after 200 µs settling time, data will modulate the carrier directly.
3. All RF protocol parts must hence be implemented in MCU firmware (preamble, address and CRC).

Direct Mode Receive:

MCU interface pins: CE, CLK1, and DATA

1. Once the nRF2401 is configured and powered up (CE high) in direct RX mode, DATA will start to toggle due to noise present on the air.
2. CLK1 will also start to toggle as nRF2401 is trying to lock on to the incoming data stream.
3. Once a valid preamble arrives, CLK1 and DATA will lock on to the incoming signal and the RF package will appear at the DATA pin with the same speed as it is transmitted.
4. To enable the demodulator to re-generate the clock, the preamble must be 8 bits toggling hi-low, starting with low if the first data bit is low.
5. In this mode no data ready (DR) signals is available. Address and checksum verification must also be done in the receiving MCU.

DuoCeiver™ Simultaneous Two Channel Receive Mode

In both ShockBurst™ & direct modes the nRF2401 can facilitate simultaneous reception of two parallel independent frequency channels at the maximum data rate. This means:

- nRF2401 can receive data from two 1 Mbps transmitters (ex: nRF2401 or nRF2402) 8 MHz (8 frequency channels) apart through one antenna interface.
- The output from the two data channels is fed to two separate MCU interfaces.
  - Data channel 1: CLK1, DATA, and DR1
  - Data channel 2: CLK2, DOUT2, and DR2
  - DR1 and DR2 are available only in ShockBurst™.

The nRF2401 DuoCeiver™ technology provides 2 separate dedicated data channels for RX and replaces the need for two, stand alone receiver systems.

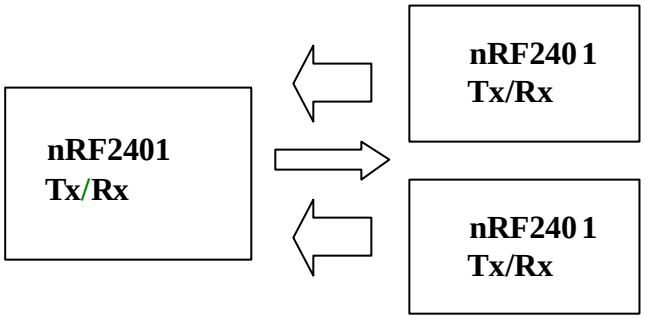


Figure 9 Simultaneous 2 channel receive on nRF2401

There is one absolute requirement for using the second data channel. For the nRF2401 to be able to receive at the second data channel the frequency channel must be 8MHz higher than the frequency of data channel 1. The nRF2401 must be programmed to receive at the frequency of data channel 1. No time multiplexing is used in nRF2401 to fulfil this function. In direct mode the MCU must be able to handle two simultaneously incoming data packets if it is not multiplexing between the two data channels. In ShockBurst™ it is possible for the MCU to clock out one data channel at a time while data on the other data channel waits for MCU availability, without any lost data packets, and by doing so reduce the needed performance of the MCU.

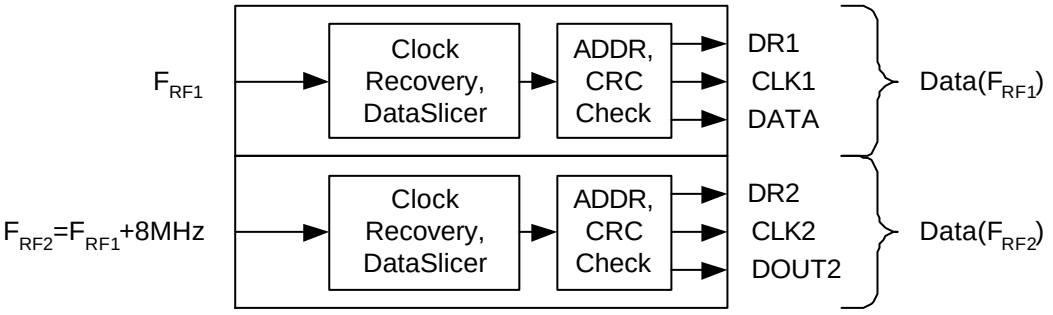
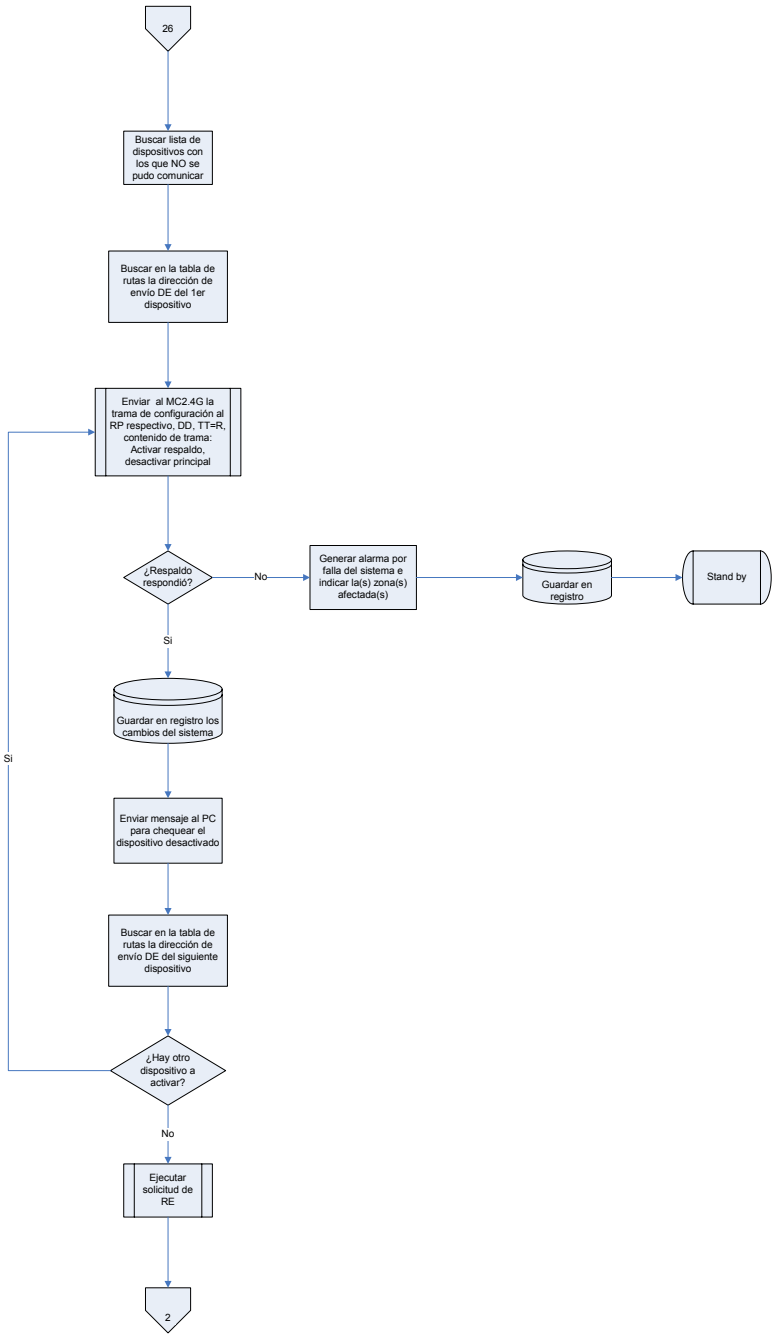


Figure 10 DuoCeiver™ with two simultaneously independent receive channels.

ANEXO 3

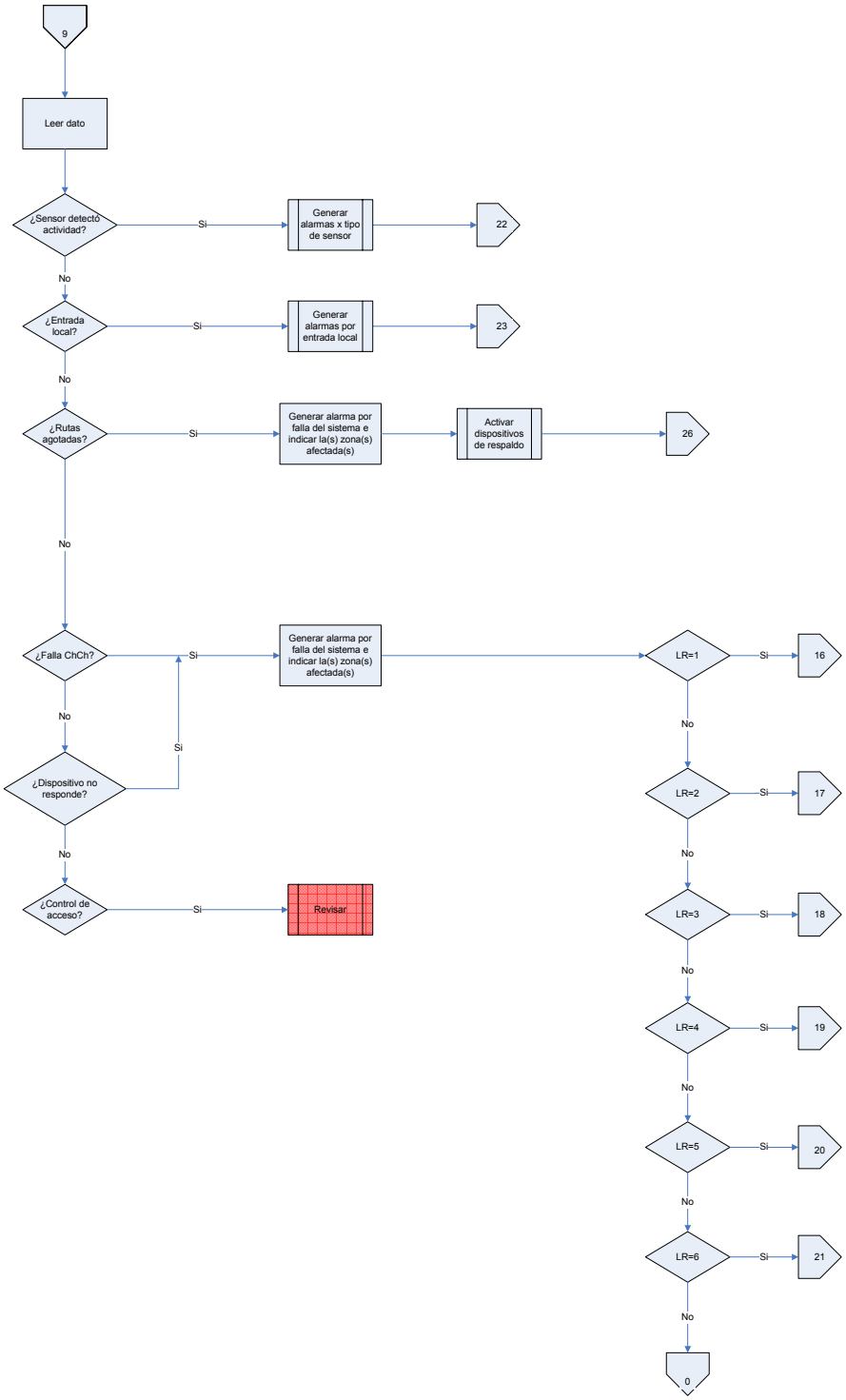
[ANEXO 3A]

Activación del sistema de respaldo



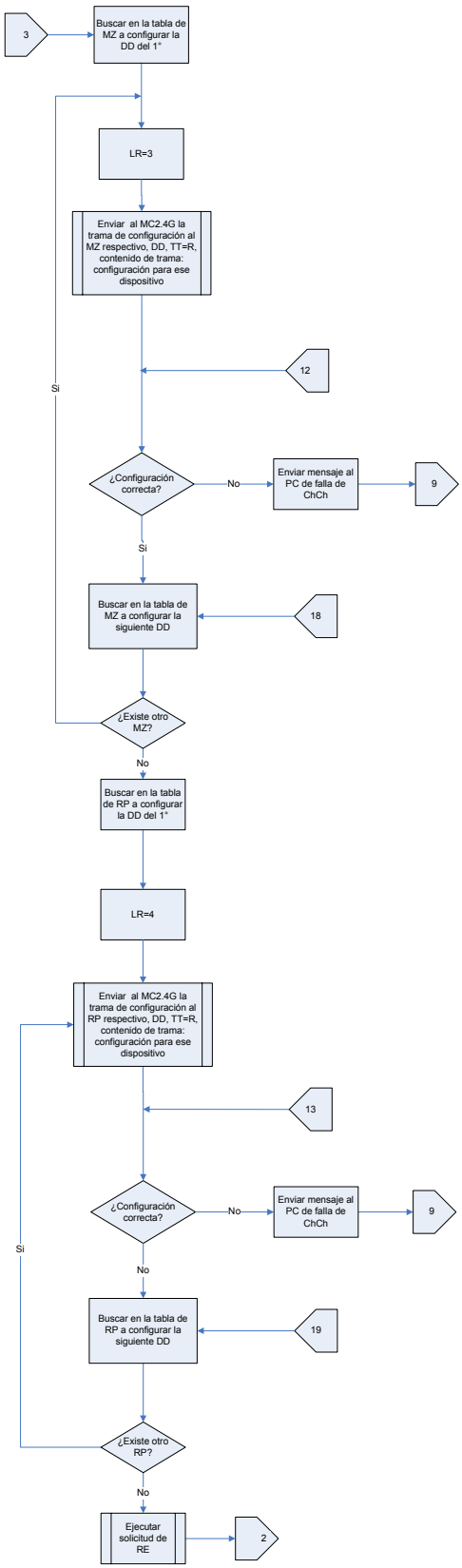
[ANEXO 3B]

Atención de alarmas



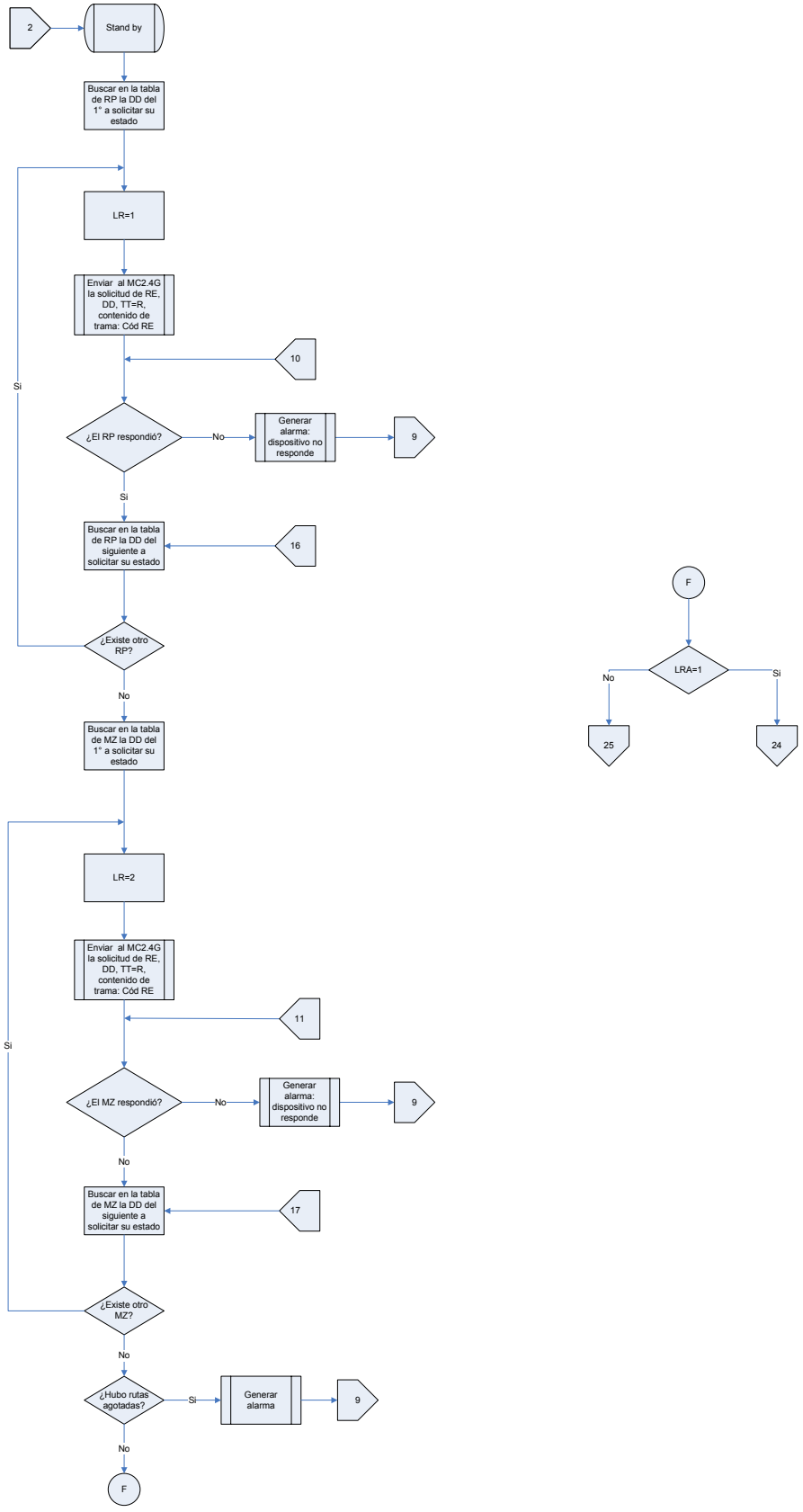
[ANEXO 3C]

Cambio de Canal



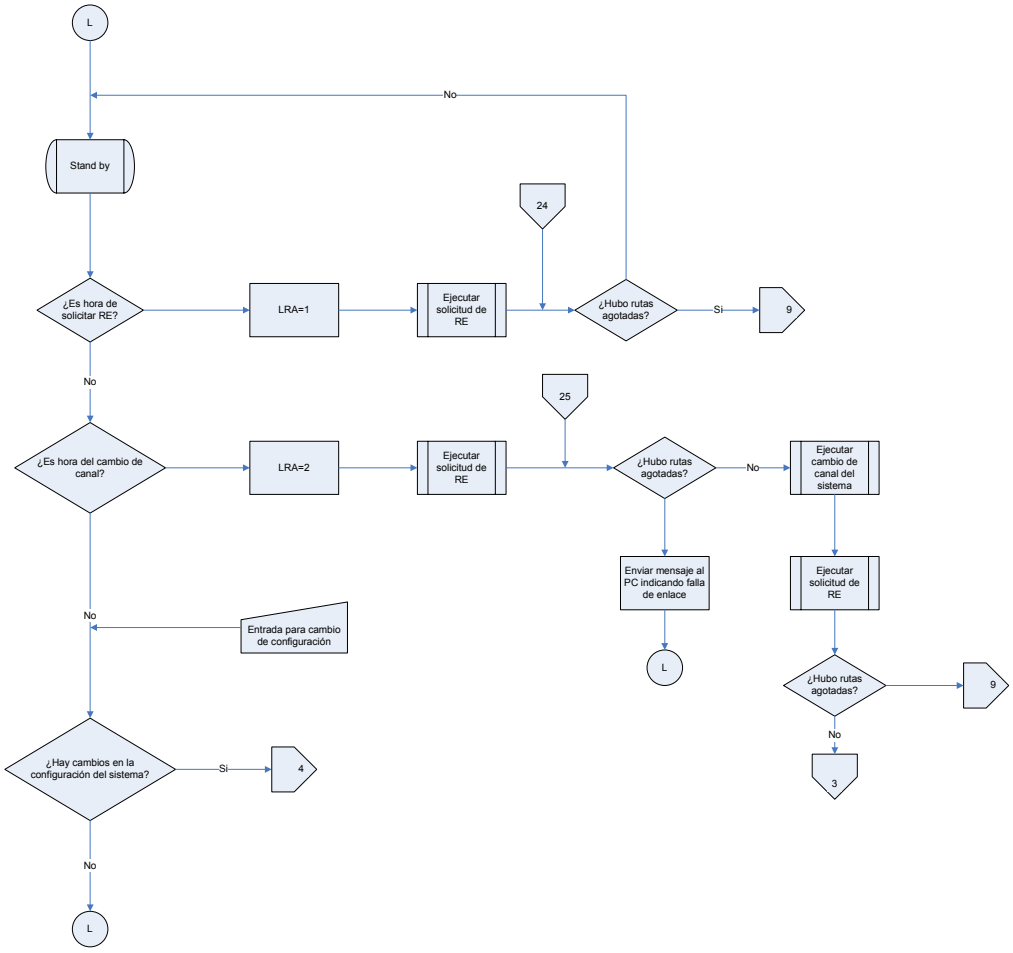
[ANEXO 3D]

Solicitud de RE



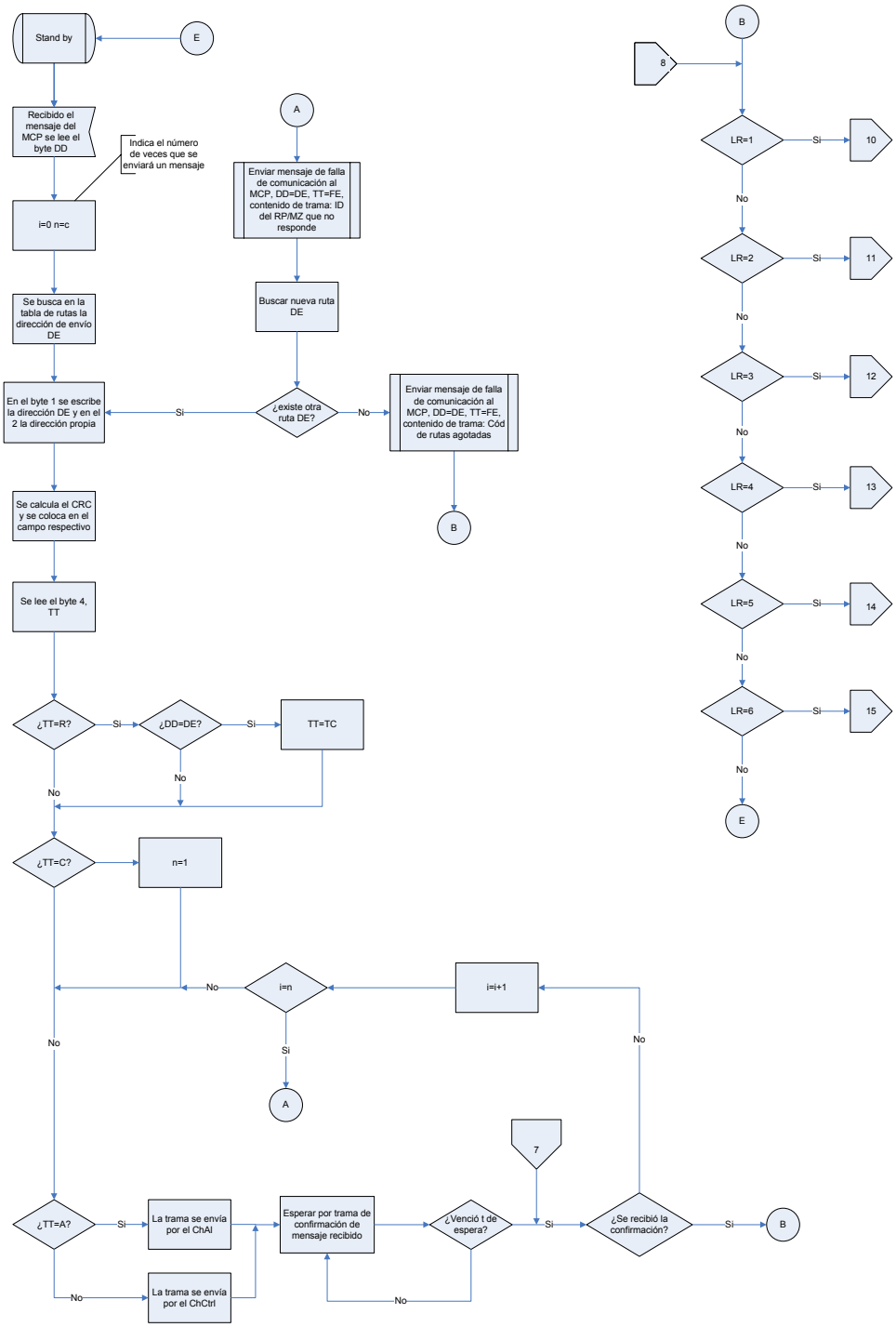
[ANEXO 3E]

Módulo de Control de Procesos
MCP-Asínc



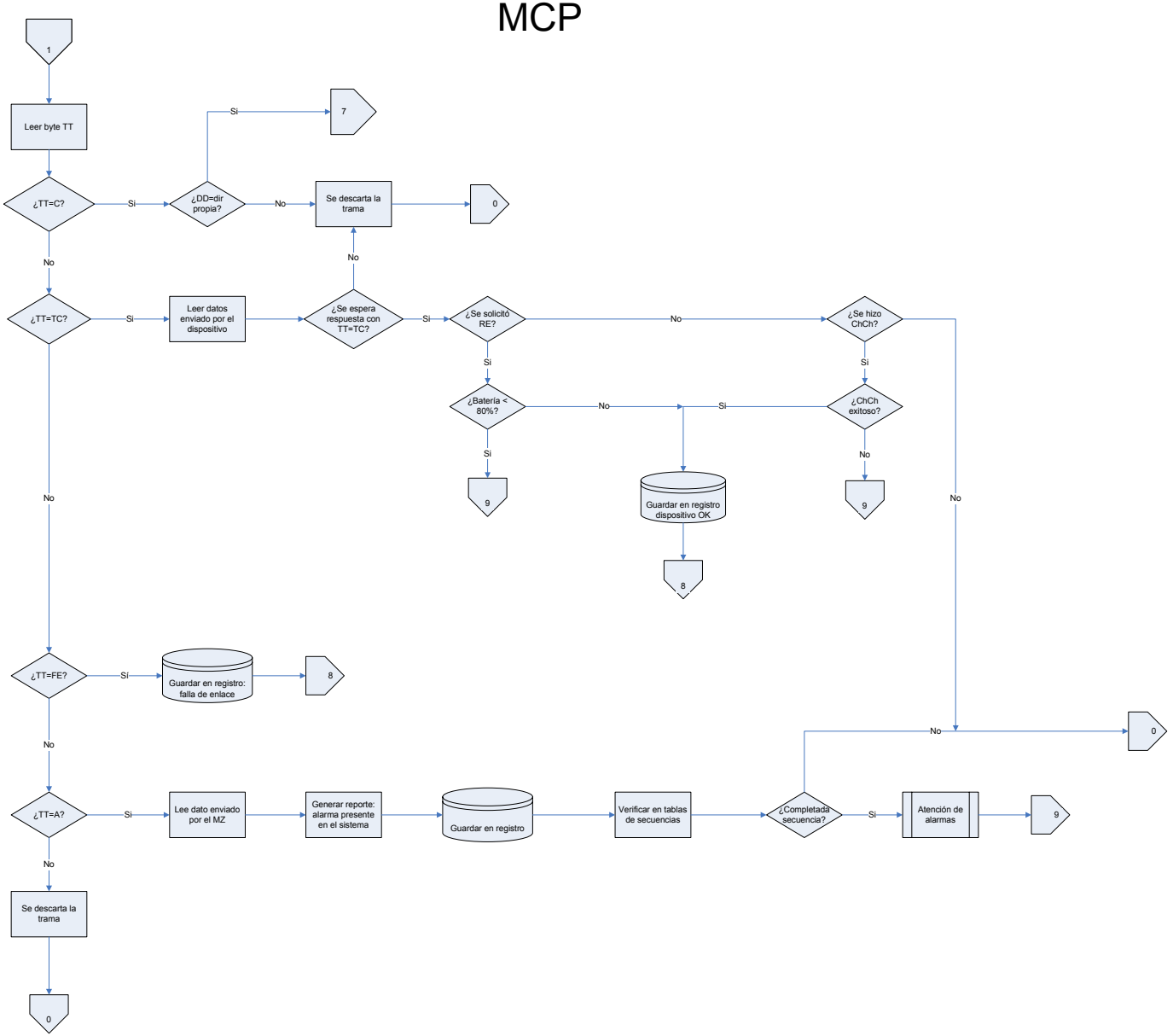
[ANEXO 3F]

Transmisor MC2.4GHz



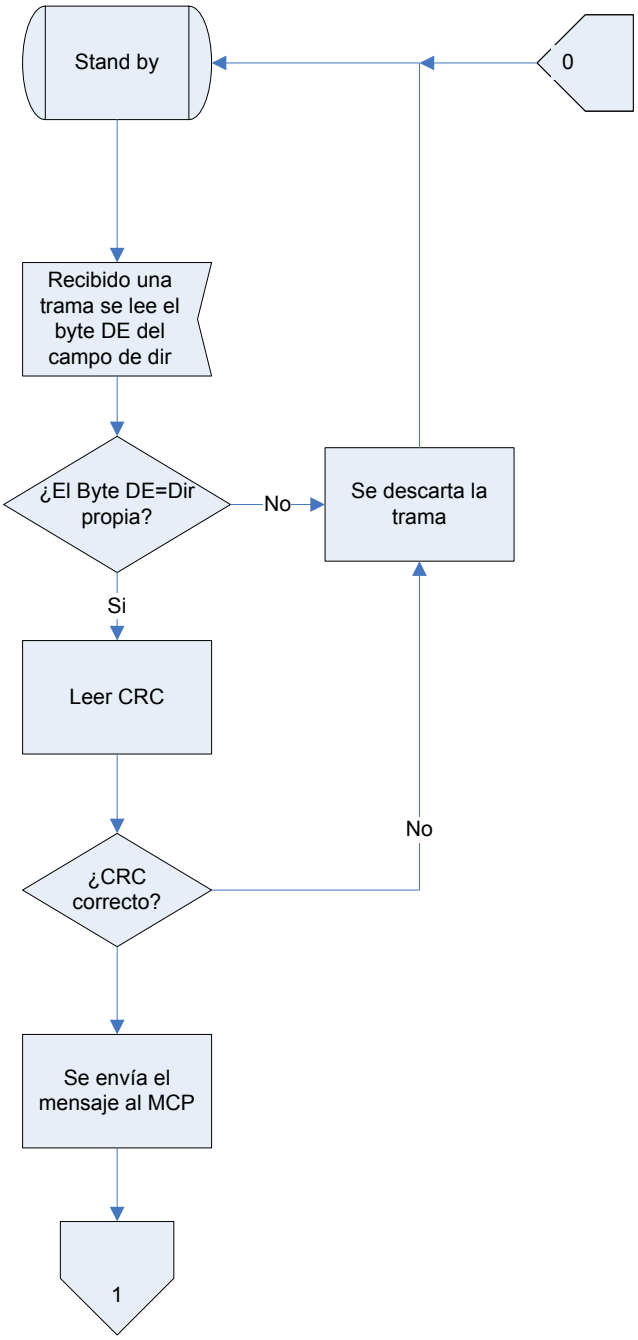
[ANEXO 3G]

Módulo de Control de Procesos
MCP



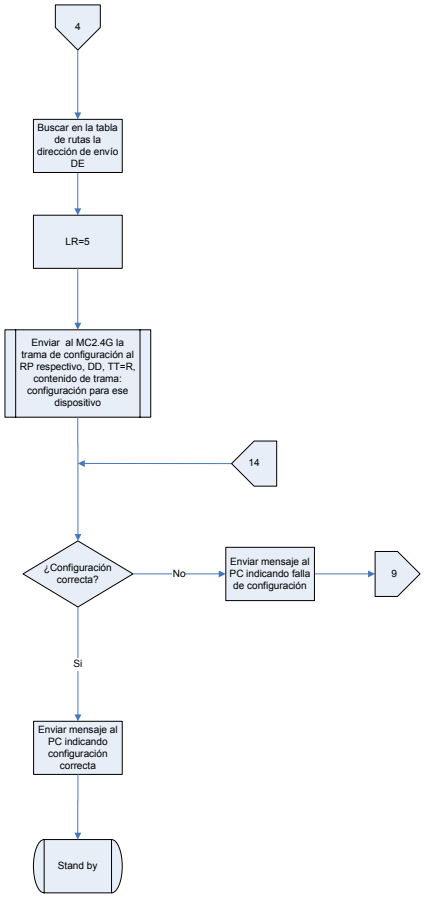
[ANEXO 3H]

Receptor del MC2.4G



[ANEXO 3I]

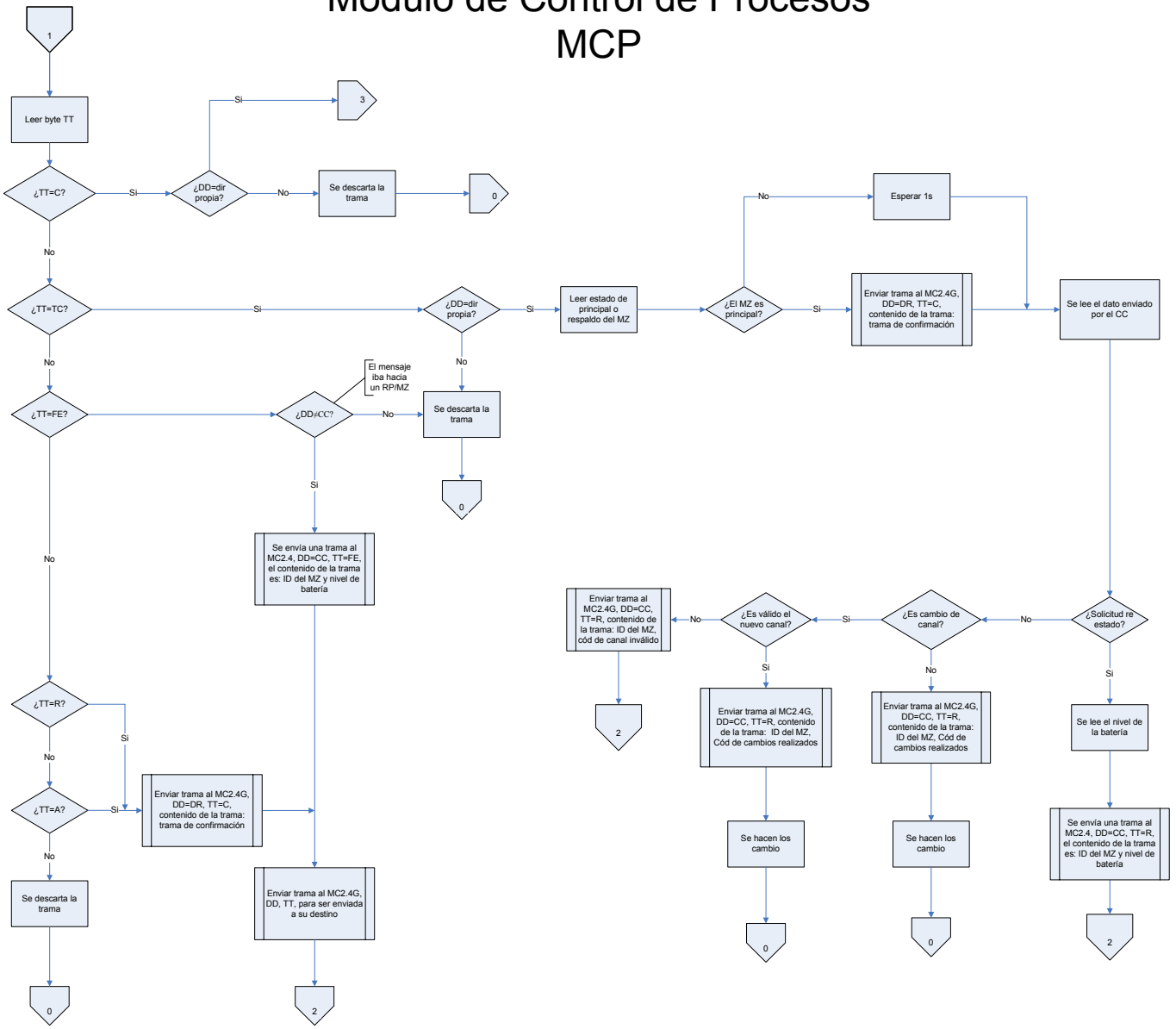
Cambio de Configuración



ANEXO 4

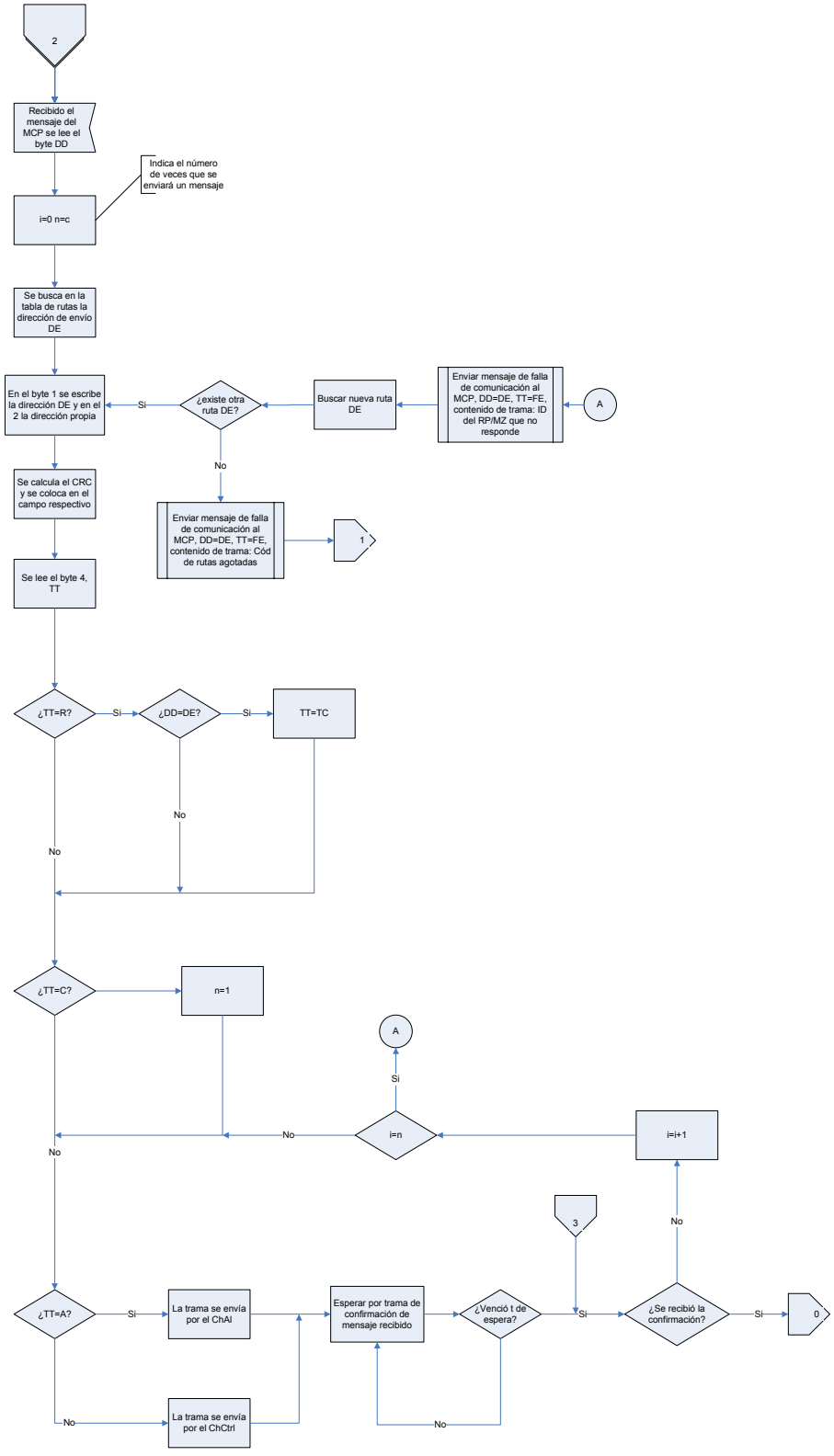
[ANEXO 4A]

Módulo de Control de Procesos MCP



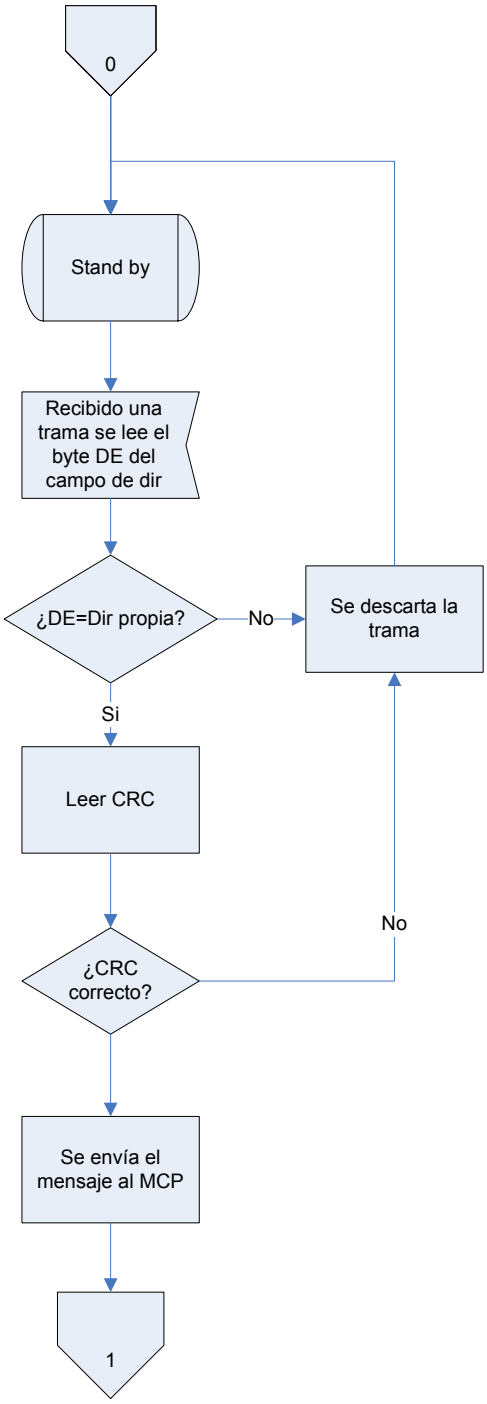
[ANEXO 4B]

Transmisor MC2.4GHz

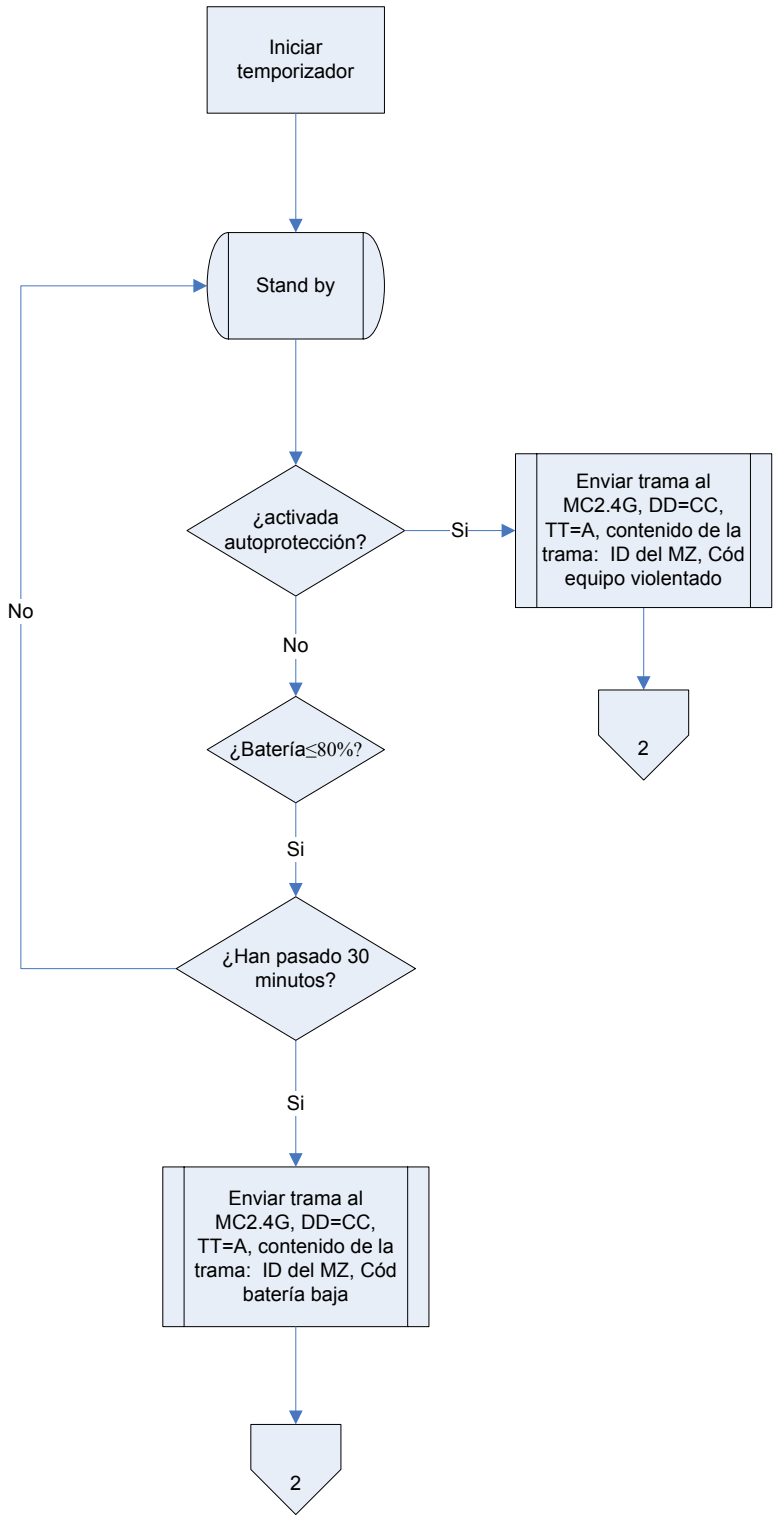


[ANEXO 4C]

Receptor del MC2.4G

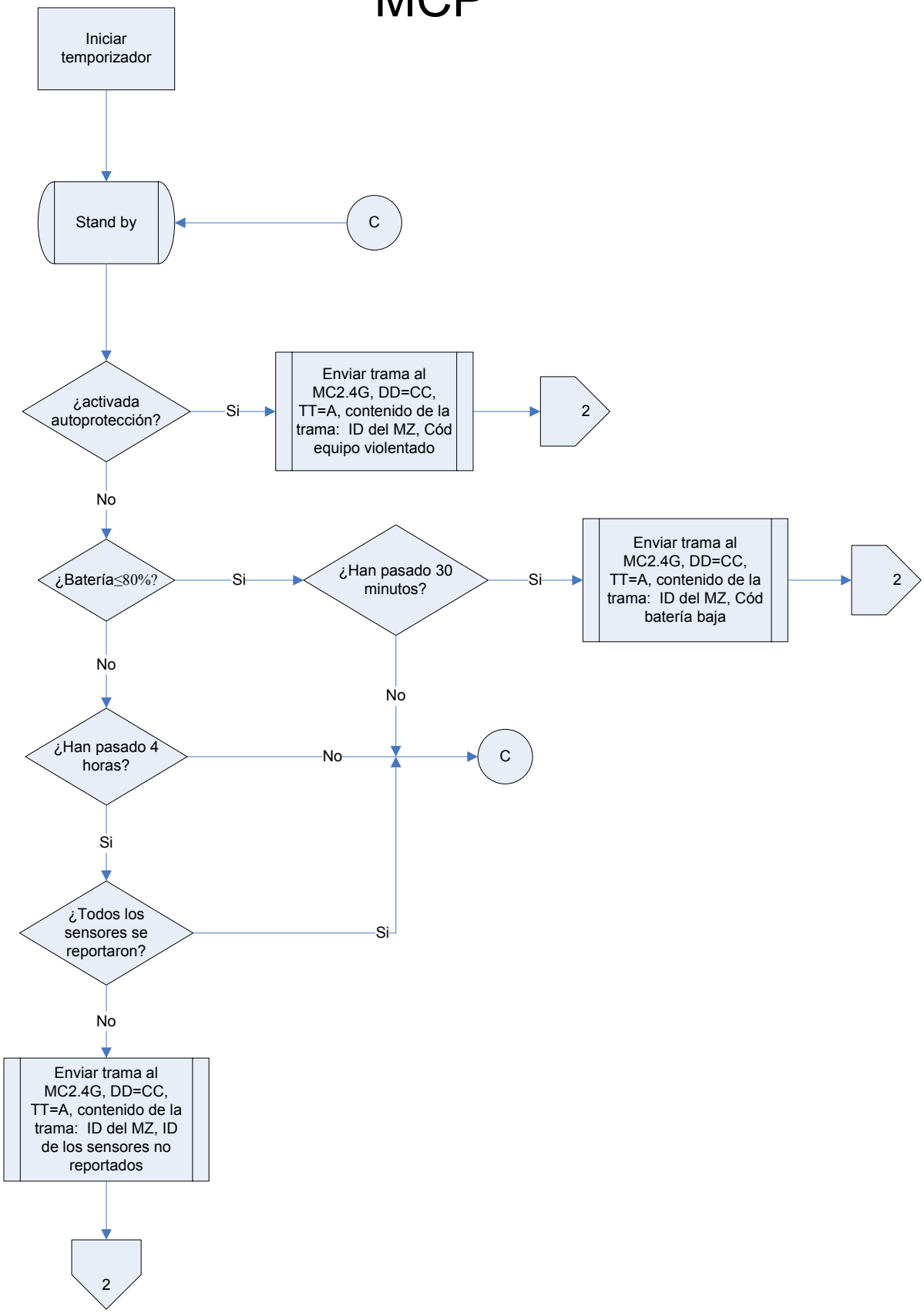


[ANEXO 4D]
Acciones asíncronas del MCP



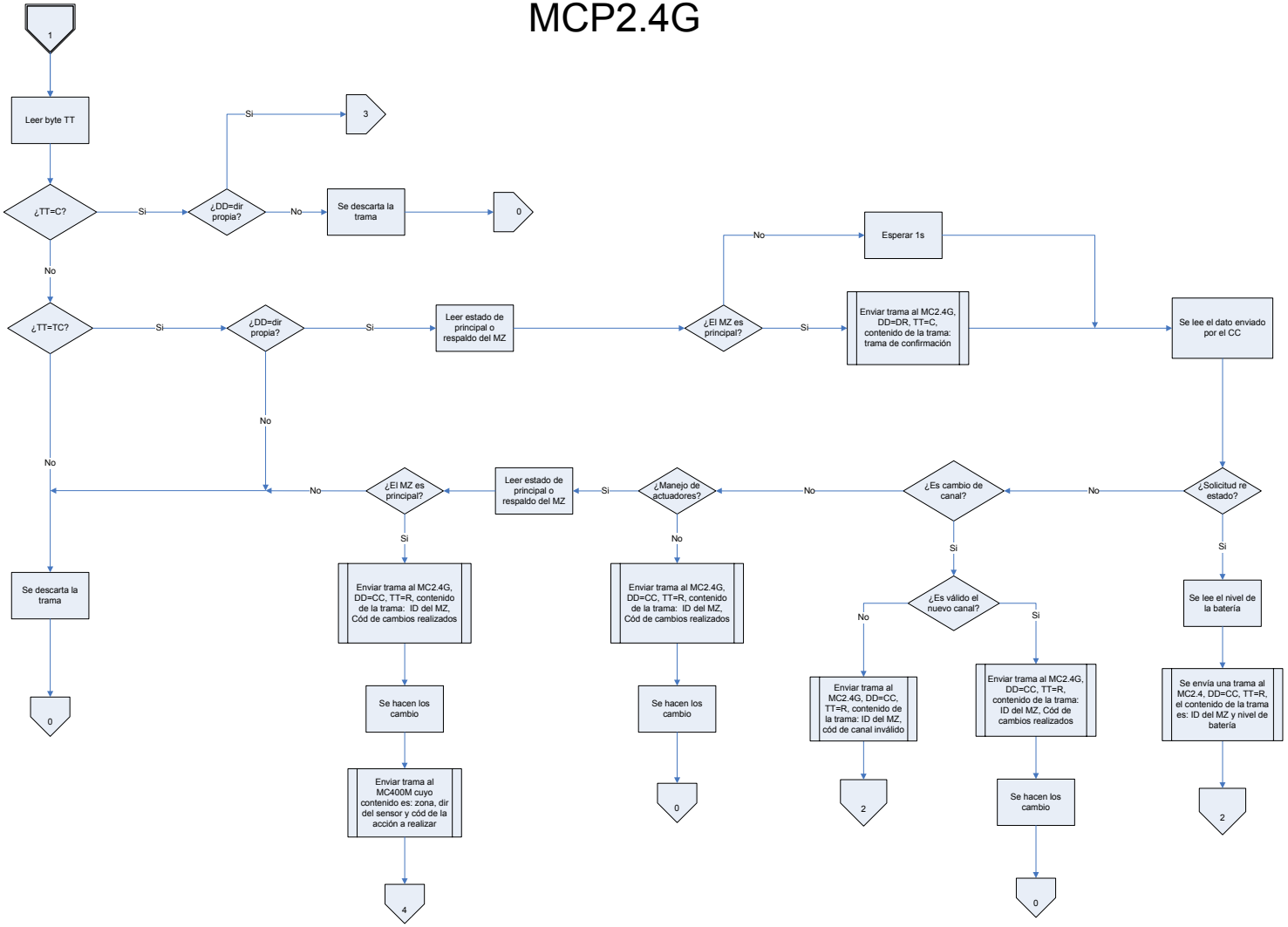
ANEXO 5

[ANEXO 5A]
Acciones asíncronas del MCP



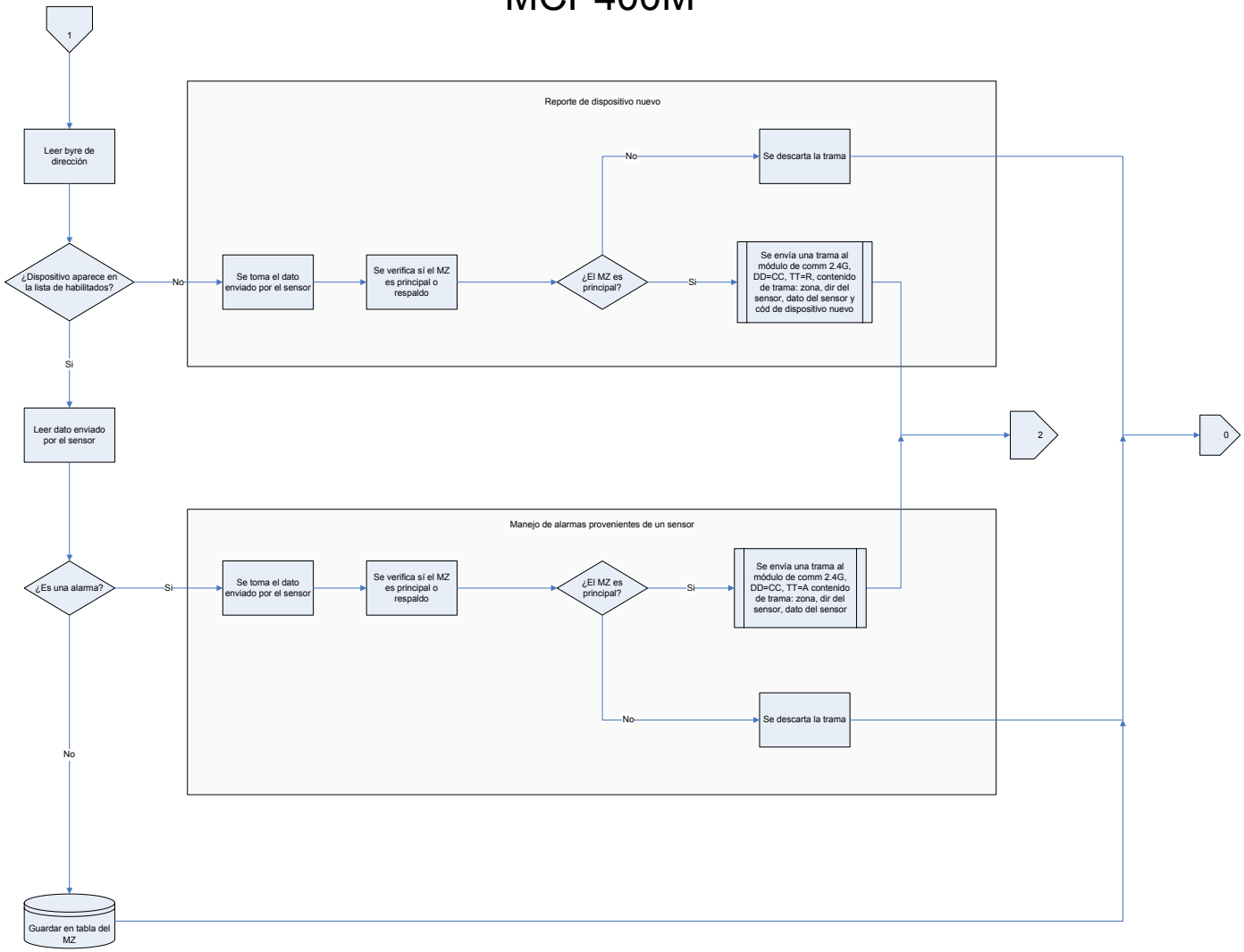
[ANEXO 5B]

Módulo de Control de Procesos
MCP2.4G



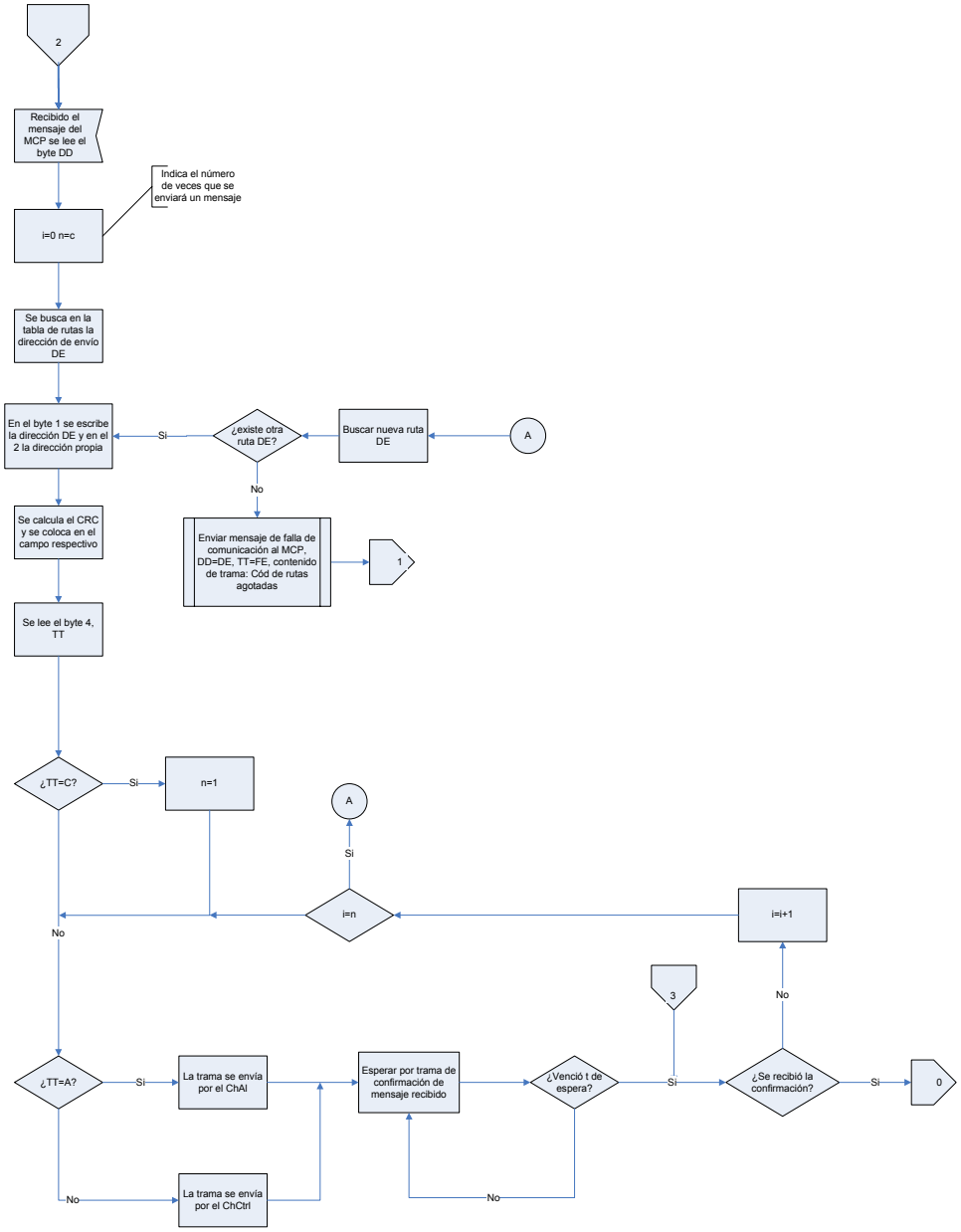
[ANEXO 5C]

Módulo de Control de Procesos
MCP400M



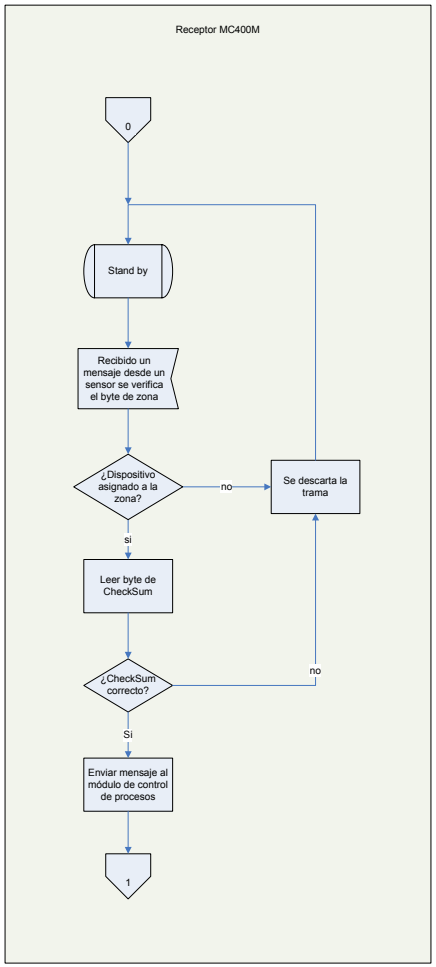
[ANEXO 5D]

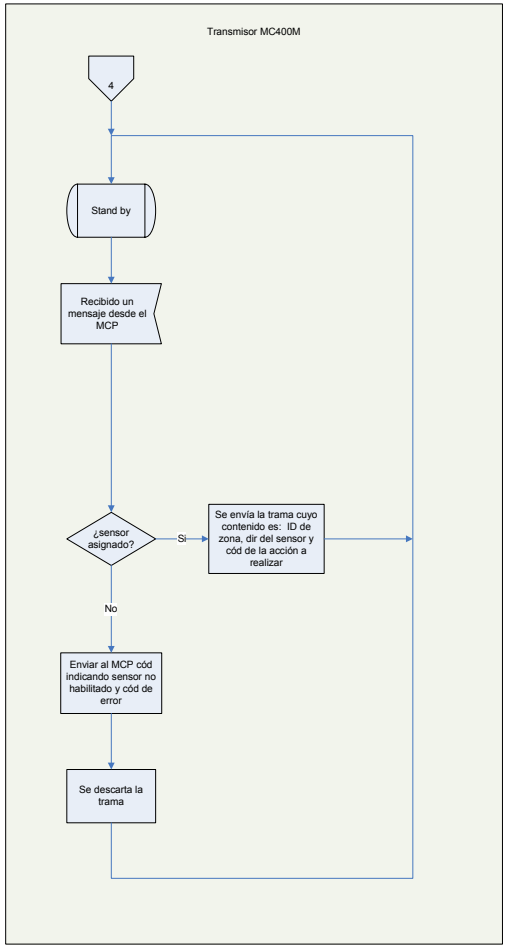
Transmisor del MC2.4G



[ANEXO 5E]

Módulo de Comunicaciones
MC400M





[ANEXO 5F]

Receptor del MC2.4G