(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 417 554**

(51) Int. CI.:

H04L 1/00 (2006.01)
G08B 25/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.06.2005 E 05757783 (5)**

(97) Fecha y número de publicación de la concesión europea: **03.04.2013 EP 1766841**

(54) Título: **Codificación híbrida de transmisiones de datos en un sistema de seguridad**

(30) Prioridad:

13.07.2004 US 891205

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.08.2013

(73) Titular/es:

HONEYWELL INTERNATIONAL INC. (100.0%)
101 Columbia Road
Morristown, NJ 07960 , US

(72) Inventor/es:

SCHMIT, THOMAS

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Codificación híbrida de transmisiones de datos en un sistema de seguridad

CAMPO TÉCNICO

Esta invención se refiere a sistemas de seguridad y otros tipos de sistemas conectados en red y en particular, al uso de sistemas de codificación de datos híbridos o múltiples para aumentar la detección y corrección de errores durante la transmisión de datos en dichos sistemas de seguridad.

ANTECEDENTES DE LA INVENCIÓN

Los sistemas de seguridad utilizados para supervisar instalaciones y determinar si se han incumplido las premisas incumplidas o existe una condición de alarma, son bien conocidos en esta técnica. Estos sistemas suelen incluir un panel de control, un medio de comunicaciones de sistemas tales como un bus de datos y varios dispositivos de seguridad situados a través de las instalaciones para realizar una determinada función en el sistema. Los dispositivos de seguridad suelen incluir sensores de ruptura de cristal, detectores de humos, detectores de incendios, sensores de movimiento, sensores de apertura de puertas y ventanas, etc. Los dispositivos de seguridad incluyen también periféricos tales como dispositivos de marcación, teclados, consolas de presentación visual, transmisores y receptores de radiofrecuencias RF, etc. El panel de control suele estar configurado para comunicarse con los dispositivos de seguridad para recoger y enviar información con estos dispositivos, tales como cuando un usuario introduce un código de “armado del sistema” en el teclado con el fin de armar el panel de control y el sistema de seguridad.

Aunque los dispositivos de seguridad, en el pasado, han sido normalmente cableados al panel de control del sistema, ha sido cada vez más común utilizar un sistema inalámbrico en donde se elimina la necesidad de un bus de datos o un bucle cableado (en su totalidad o en parte) utilizando comunicaciones de radiofrecuencias (RF) entre componentes. En particular, es deseable utilizar un transmisor de RF en conjunción con un dispositivo de seguridad, tal como un detector de movimiento para transmitir señales de RF a un receptor de RF situado cerca o integrado con el panel de control para efectuar comunicaciones inalámbricas entre el dispositivo de seguridad y el panel de control. El receptor de RF puede estar también interconectado a un bucle o bus cableado (al que está unido el panel de control), de modo que se utiliza un enlace inalámbrico entre el dispositivo de seguridad y el resto del sistema de seguridad (cableado).

La integridad de datos es una preocupación particular con los sistemas de seguridad inalámbricos, puesto que no existe ninguna conexión cableada entre el dispositivo de seguridad y el panel de control. En el pasado, se han utilizado métodos, tales como un control de redundancia cíclica (CRC), en un intento de proporcionar alguna detección y/o corrección de errores en las transmisiones de datos. Es un objetivo de la presente invención dar a conocer una metodología mejorada para garantizar transmisiones de datos libres de errores entre componentes de un sistema de seguridad.

El documento US-A-2004/0066935 da a conocer un sistema de seguridad y su protocolo inalámbrico en donde el mensaje incluye un campo de tipo de producto dentro de un número de identificación/serie. El mensaje puede incluir también una cuenta de secuencia.

El documento WO-A-97/08864 da a conocer un método para decodificar mensajes transmitidos en donde una repetición codificada de la palabra de datos se compila seleccionando bits a partir de una pluralidad de repeticiones codificadas recibidas.

SUMARIO DE LA INVENCIÓN

En consecuencia, la presente invención es un sistema de seguridad que tiene dispositivos de seguridad que se comunican, de forma inalámbrica, con un panel de control a través de un receptor. Cada dispositivo de seguridad tiene un transmisor de RF asociado. En primer lugar, un mensaje de datos en dos partes se forma en el dispositivo de seguridad/transmisor, que tiene una primera parte de mensaje y una segunda parte de mensaje. La primera parte de mensaje incluye una parte de preámbulo, una parte de número de identificación que identifica, de forma única, el dispositivo de seguridad, una parte de estado que comprende datos de estado o de mensaje indicativos del estado del dispositivo de seguridad y una parte de CRC que contiene datos de CRC basados en una función de CRC realizada en la parte del número de identificación y la parte de estado. La segunda parte de mensaje puede incluir diferentes tipos de datos, dependiendo de la funcionalidad deseada, según aquí se describe. La primera parte de mensaje se codifica utilizando un primer formato de codificación (que suele ser un formato de reposición a cero (RZ)) y la segunda parte de mensaje se codifica en un segundo formato de codificación diferente del primer formato de codificación, (que suele ser un formato de no reposición a cero (NRZ)). A continuación, se modula una señal portadora (tal como mediante una modulación en amplitud) con la primera parte de mensaje codificada y la segunda parte de mensaje codificada y se transmite la señal portadora modulada.

En un primer aspecto de la presente invención, la segunda parte de mensaje incluye una primera parte de estado redundante que repite los datos de estado desde la primera parte de mensaje y una segunda parte de estado redundante

que repite también los datos de estado desde la primera parte de mensaje, pero es la inversa lógica de la primera parte de estado redundante. Un dispositivo receptor, tal como un receptor autónomo o un receptor integrado con un panel de control, recibe la señal transmitida y la demodula consecuentemente. El dispositivo receptor decodifica, entonces, la primera parte de mensaje utilizando el primer formato de codificación (RZ) para obtener la parte de preámbulo, la parte de número de identificación, la parte de estado y la parte de CRC. La segunda parte de mensaje se decodifica utilizando el segundo formato de codificación (NRZ) para obtener la primera parte de estado redundante y la segunda parte de estado redundante.

A continuación, los circuitos de procesamiento se utilizan para analizar los datos recibidos, en particular, para analizar dos o más de la parte de estado, la primera parte de estado redundante, la segunda parte de estado redundante y la parte de CRC, con el fin de determinar si el mensaje ha sido válidamente recibido. A modo de ejemplo, en un método relativamente sencillo, la parte de estado se compara con la primera parte de estado redundante y si la parte de estado es la misma que la primera parte de estado redundante, entonces el mensaje se etiqueta como siendo válidamente recibido. Como alternativa, la parte de estado puede compararse con la segunda parte de estado redundante y si la parte de estado es la misma que la segunda parte de estado redundante, entonces el mensaje se etiqueta como siendo válidamente recibido. De forma análoga, la parte de estado puede compararse con la primera parte de estado redundante y la segunda parte de estado redundante y si todas ellas son las mismas, entonces el mensaje se etiqueta como siendo válidamente recibido.

Si así se desea, pueden seguirse escenarios operativos más sofisticados. A modo de ejemplo, se puede generar un CRC en función de la parte de número de identificación y de la parte de estado y el CRC generado puede compararse con la parte de CRC desde el mensaje recibido. Si el CRC generado es el mismo que la parte de CRC desde el mensaje recibido, entonces, el mensaje se etiqueta como siendo válidamente recibido. Si, sin embargo, el CRC generado no es el mismo que la parte de CRC del mensaje, entonces se puede realizar un análisis adicional, en donde la parte de estado puede compararse con la primera parte de estado redundante y la segunda parte de estado redundante y si son las mismas, entonces el mensaje se etiqueta como siendo válidamente recibido. Otros escenarios operativos de análisis, que utilizan estas partes de mensajes recibidas, se describen a continuación.

En un segundo aspecto de la presente invención, la segunda parte de mensaje incluye información de secuencia que es indicativa del secuenciamiento relativo de mensajes desde el dispositivo de seguridad para prestar asistencia al dispositivo receptor (p.e., el panel de control) al determinar si el mensaje se ha recibido fuera de orden y debe ignorarse. En particular, la segunda parte de mensaje incluye una primera cuenta de secuencia y una segunda cuenta de secuencia que tiene la misma información que la primera cuenta de secuencia, pero es su inversa lógica. El dispositivo receptor, según se describió anteriormente, decodificada la primera parte de mensaje utilizando el primer formato de codificación (RZ) para obtener la parte de preámbulo, la parte de número de identificación, la parte de estado y la parte de CRC. La segunda parte de mensaje se decodifica utilizando el segundo formato de codificación (NRZ) para obtener la cuenta de secuencia. Los circuitos de procesamiento se utilizan, entonces, para analizar los datos recibidos, en particular para comparar la cuenta de secuencia desde el mensaje con una cuenta de secuencia anterior desde la memoria. Si la cuenta de secuencia desde el mensaje es menor o igual a la cuenta de secuencia anterior, entonces se ignora el mensaje. Si, sin embargo, la cuenta de secuencia desde el mensaje no es menor ni igual a la cuenta de secuencia anterior, entonces, se procesa el mensaje y la cuenta de secuencia anterior se sustituye, en memoria, con la cuenta de secuencia desde el mensaje. La cuenta de secuencia y la cuenta de secuencia inversa son analizadas ambas con respecto entre sí para garantizar la integridad de datos.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 es un diagrama de bloques de un sistema de seguridad típico;

La Figura 2 es un diagrama de bloques del procesamiento de mensaje de datos en el transmisor de un primer aspecto de esta invención;

La Figura 3 es un diagrama de bloques del procesamiento de mensajes de datos en el dispositivo receptor de un primer aspecto de esta invención;

La Figura 4 es una ilustración de un formato de datos RZ y NRZ según se utiliza en esta invención y

Las Figuras 5A, 5B, 5C, 5D, 5E y 5F ilustran, cada una, diagramas de flujo de análisis de datos alternativos utilizados en el primer aspecto de esta invención;

La Figura 6 es un diagrama de bloques del procesamiento de mensajes de datos en el transmisor de un segundo aspecto de esta invención;

La Figura 7 es un diagrama de bloques del procesamiento de mensajes de datos en el dispositivo receptor de un segundo aspecto de esta invención;

Las Figuras 8 y 9 son diagramas de flujo de la operación del segundo aspecto de esta invención.

FORMA DE REALIZACIÓN PREFERIDA DE LA INVENCIÓN

La forma de realización preferida del primer aspecto de la presente invención se describe ahora con referencia a las Figuras. La Figura 1 ilustra un sistema de seguridad 2 típico que incluye varios dispositivos de seguridad 4, 6, 8, enviando, cada uno de ellos, transmisiones de datos de radiofrecuencias RF 14, 16, 18 a un módulo receptor 10 y un panel de control asociado 12 según se conoce en esta técnica. Según se indicó anteriormente, los dispositivos de seguridad 4, 6, 8, pueden ser cualquier dispositivo que se utilice en un sistema de seguridad incluyendo, sin limitación, a sensores de ruptura de cristal, detectores de humos, detectores de incendios, sensores de movimiento PIR, sensores de movimiento de microondas, sensores de apertura de puertas y ventanas, dispositivos de marcación, teclados, consolas de presentación visual y dispositivos similares. El dispositivo de seguridad puede ser también una pasarela, un adaptador o una interfaz entre el panel de control y otro dispositivo. A modo de ejemplo, es común tener un receptor de RF conectado a un bus de comunicaciones cableado (o bucle) al que está conectado el panel de control. El receptor de RF recibe mensajes desde otro dispositivo de seguridad, tal como un sensor de PIR inalámbrico (puede ser también un transmisor de RF para enviar mensajes al sensor PIR inalámbrico). En este caso, el receptor de RF (y/o transmisor de RF) así como los sensores inalámbricos se consideran como dispositivos de seguridad en el alcance de protección de esta invención.

El panel de control 12 actúa como el controlador del sistema para el sistema de seguridad y proporciona varias funciones tales como armado y desarmado del sistema, supervisión de los dispositivos de seguridad, aceptación de mensajes desde los dispositivos de seguridad para determinar si existe una condición de alarma, haciendo que suene una alarma, etc. El receptor 10 puede estar separado o integrado con el panel de control 12. Además, el procesamiento y el análisis de los mensajes de datos recibidos, según aquí se describe, pueden realizarse en el receptor 10 o en el panel de control 12, según se configure por el diseñador del sistema.

Los dispositivos de seguridad pueden tener transmisores de RF integrados, como en la forma de realización preferida, o dichos transmisores pueden estar separados del dispositivo de seguridad (pero en estrecha proximidad y cableado). La Figura 2 ilustra la funcionalidad del dispositivo de seguridad con un transmisor de RF integrado. Un mensaje de datos 28 que ha de enviarse al panel de control, se forma y está constituido por dos partes principales. La parte 1 del mensaje de datos 28, según se ilustra en la Figura 2, es similar a la que se conoce en la técnica e incluye una parte de preámbulo 30, una parte de identificación 32 (que identifica, de forma única, el dispositivo de seguridad tal como un número serie), una parte de estado 34 y una parte de CRC 36. La parte de estado 34 incluye bits que son de principal interés para el panel de control e incluye bits que indican el estado operativo del dispositivo de seguridad, nivel de la batería, etc. El CRC se genera, según se conoce en esta técnica, como una función de la parte de identificación ID 32 y la parte de estado 34 y se ha utilizado, con anterioridad, como un medio de detección de errores por el panel de control/receptor. La presente invención mejora en el uso de solamente el CRC como dispositivo adicional aquí descrito.

Una segunda parte de mensaje se forma según esta invención y se ilustra en la Figura 2 como parte 2 del mensaje 28. La parte 2 incluye una primera parte de estado redundante 38, que es simplemente los mismos datos que la parte de estado 34 en la parte 1. La parte 2 incluye, además, una segunda parte de estado redundante 40, que transmite también la misma información que la parte de estado 34 de la parte 1, pero que es la inversa lógica de la primera parte de estado 38. Invirtiendo la segunda parte de estado redundante 40, una amplitud media constante se mantiene durante la segunda parte completa del mensaje (p.e., cuando se utiliza la modulación en amplitud). Es decir, si la parte de estado 34 (y la primera parte de estado redundante 38) es, a modo de ejemplo, 1101101000101010, entonces, la segunda parte de estado redundante será 0010010111010101.

El mensaje de datos 28 se codifica, entonces, para la transmisión como sigue. La parte 1 del mensaje se codifica en un formato de reposición a cero (RZ) con un codificador de RZ 42 y la parte 2 del mensaje se ilustra en un formato de no reposición a cero (NRZ) con un codificador NRZ 44. El formato RZ, según se ilustra en lado izquierdo de la Figura 4, es también conocido como el método de codificación Manchester (la codificación Manchester se define como un código en el que (a) señales de datos y reloj se combinan para formar un flujo de datos de sincronización automática único, (b) cada bit codificado contiene una transición en el punto medio de un periodo de bits, (c) la dirección de transición determina si el bit es “0” o “1” y (d) la primera mitad es el complemento del valor de bit verdadero y la segunda mitad es el valor de bit verdadero). El formato de NRZ, ilustrado en lado derecho de la Figura 4, no requiere que la señal de datos efectúe una reposición a cero entre bits. De este modo, el nivel lógico 1 se muestra como una tensión positiva y el nivel lógico 0 se muestra como una tensión cero. En el formato de NRZ, la señal no es autosincronizada como con el formato de RZ. Sin embargo, codificando la segunda parte del mensaje con el formato de NRZ inmediatamente después de la primera parte de mensaje que utiliza la codificación de RZ, la señal de reloj que ha sido derivada desde la parte de RZ puede extrapolarse y utilizarse para sincronizar los datos en la parte de NRZ. Lo anterior no puede ser factible si la señal fue codificada completamente en el formato de NRZ, puesto que no había ningún reloj disponible.

Además, puesto que transporta menos información de temporización, el uso de la técnica de RZ minimiza el tiempo de transmisión adicional (“en el aire”) y el ancho de banda de canal requerido para transmitir la información de estado redundante en la segunda parte de mensaje. Además, el uso de la codificación de RZ complementa la codificación de NRZ. Debido a su estructura simétrica y redundante, la primera parte codificada de RZ del mensaje proporciona una mejora en el rendimiento de decodificación relativa a NRZ bajo determinadas condiciones del canal y viceversa. La

misma ventaja se aplica a las diferencias en los métodos de decodificación entre RZ y NRZ según se describe a continuación.

Existen dos ejemplos de los formatos de RZ y de NRZ que pueden utilizarse en la presente invención. Otros tipos pueden utilizarse también y siguen proporcionando las ventajas aquí descritas.

Después de que se hayan codificado los datos en la forma descrita, el flujo de datos se utiliza para modular una señal portadora de RF y se transmite como es conocido en esta técnica. A modo de ejemplo, un sistema de modulación en amplitud (AM) puede utilizarse como es conocido en esta técnica.

La señal modulada se recibe y demodula por el dispositivo receptor, según se ilustra en la Figura 3 y según es bien conocido en esta técnica. A continuación, la señal se decodifica utilizando el decodificador RZ 62 y el decodificador de NRZ 60 para obtener el mensaje de datos recibido 64, según se ilustra en la Figura 3. A continuación, se realiza un análisis del mensaje recibido 64 con el fin de averiguar si la señal fue exactamente recibida y debe procesarse, además, como un mensaje válidamente recibido. El bloque de análisis de datos 78 utilizará la parte de estado 70, la parte de CRC 72, la primera parte de estado redundante 74 y la segunda parte de estado redundante 76 en una o más diversas maneras para averiguar la validez del mensaje recibido 64. Las Figuras 5A – 5F ilustran el flujo de análisis utilizado en la presente invención.

La Figura 5A ilustra cómo se compara la parte de estado 70 con la primera parte de estado redundante 74. SI la parte de estado 70 es la misma que la primera parte de estado redundante 74, entonces, el mensaje 64 se etiqueta como siendo válidamente recibido. Como alternativa, según se ilustra en la Figura 5B, la parte de estado 70 puede compararse con la segunda parte de estado redundante 76. Si la parte de estado 70 es la misma que la segunda parte de estado redundante 76, entonces, el mensaje se etiqueta como siendo válidamente recibido. De forma análoga, según se ilustra en la Figura 5C, la parte de estado 70 puede compararse con la primera parte de estado redundante 74 y la segunda parte de estado redundante 76 y si todas ellas son las mismas, entonces el mensaje se etiqueta como siendo válidamente recibido.

Si así se desea, pueden seguirse escenarios operativos más complicados. A modo de ejemplo, según se ilustra en la Figura 5D, se puede generar un CRC basado en la parte de número de identificación 68 y la parte de estado 70 y el CRC generado puede compararse con la parte de CRC 72 desde el mensaje recibido 64. Si el CRC generado es el mismo que la parte de CRC desde el mensaje, entonces, el mensaje se etiqueta como siendo válidamente recibido. Si, sin embargo, el CRC generado no es el mismo que la parte de CRC desde el mensaje, entonces, la parte de estado puede compararse con la primera parte de estado redundante y la segunda parte de estado redundante y si son las mismas, entonces, el mensaje se etiqueta como siendo válidamente recibido.

La Figura 5E ilustra un ejemplo adicional del análisis realizado por el bloque de análisis 78. En primer lugar, la primera parte de estado redundante 74 y la segunda parte de estado redundante 76 se compara y si son las mismas, entonces, se comparan con la parte de estado 70. El mensaje se etiqueta como siendo válidamente recibido cuando pasa esta comparación.

La Figura 5F ilustra otra forma de realización, a modo de ejemplo, de análisis de datos. En primer lugar, se genera un CRC en función de la parte de número de identificación 68 y de la parte de estado 70. El CRC generado se compara con la parte de CRC 72 desde el mensaje recibido. Si son las mismas, entonces, la primera parte de estado redundante 74 se compara con la segunda parte de estado redundante 76 y si son las mismas, entonces el mensaje se etiqueta como siendo válidamente recibido. Si, sin embargo, el CRC generado no es el mismo que la parte de CRC 72 desde el mensaje, entonces, la primera parte de estado redundante se compara con la segunda parte de estado redundante y si son las mismas, entonces, se genera un segundo CRC sobre el número de identificación 68 y la primera parte de estado redundante 74, el segundo CRC generado se compara con la parte de CRC 72 desde el mensaje y si pasa la comparación, entonces, la primera parte de estado redundante se utiliza como una parte de estado válidamente recibida (si falla la comparación, entonces el mensaje se etiqueta como siendo recibido de forma no válida).

De este modo, debido a la presencia de la información de estado redundante, el dispositivo receptor puede realizar una determinación en cuanto a la exactitud del mensaje recibido y proceder en consecuencia (p.e., utilizar el mensaje o desecharlo). Incorporando la información redundante en una segunda parte del mensaje que se codifica en un formato diferente que la primera parte, se consigue una metodología de transmisión sólida que proporcionará una mayor posibilidad de transmisión exacta en entornos variables, en donde una metodología de codificación puede actuar mejor que la otra.

Haciendo referencia a las Figuras 6, 7, 8 y 9, el segundo aspecto de la invención utiliza el mismo sistema de codificación híbrida del primer aspecto de la invención, pero en lugar de transmitir datos de estado redundante en la segunda parte de mensaje, se transmite información de secuencia del mensaje. En conformidad con este segundo aspecto de la invención, se solucionan los problemas asociados con tener múltiples receptores recibiendo mensajes desde el mismo transmisor, en diferentes momentos. Si una instalación requiere que más de dos receptores de RF deben distribuirse en posiciones estratégicas a través de todo el sistema y conectarse a un control de seguridad único a través de un bus de comunicación único, el uso de la información de secuencia en la señal transmitida permitirá al panel de control procesar

adecuadamente las señales recibidas. Para aclarar esta cuestión, se supone un número de secuencia de ocho bits contenido dentro de la información de señal transmitida, que se avanza en un incremento, en un transmisor dado, cada vez que el transmisor ha de emitir un nuevo evento operativo. El nuevo evento operativo puede ser la apertura de una puerta o el cierre de esa misma puerta. Se supone, además, que tarda de 2 a 4 segundos el transmisor en repetir el número requerido de mensajes de "apertura" o "cierre" idénticos por evento operativo. Si la puerta se abre y cierre dentro del intervalo de tiempo de 2 a 4 segundos, es posible para el panel de control recibir los informes de apertura y cierre desde un receptor de RF y solamente el informe de apertura desde otro receptor, que puede estar en un alcance marginal desde el transmisor dado. Sin una cuenta de secuencia incluida como parte de los eventos operativos transmitidos, el control podría determinar, de forma errónea, el estado final de la puerta a abrirse en lugar de cerrarse si se procesa el evento de apertura inicial desde el segundo receptor después del procesamiento del evento operativo de cierre desde el primer receptor. Cuanto mayor sea el número de receptores utilizados en el bus de control común, tanto mayor sería la probabilidad de este tipo de error de control. Con una cuenta de secuencia incluida en los mensajes transmitidos, como en la presente invención, la cuenta del evento operativo de apertura sería más baja que la del evento operativo de cierre, puesto que el evento operativo de apertura precedió al evento operativo de cierre, lo que indica al control que debe cerrarse el estado final de esa puerta.

Haciendo referencia al diagrama de bloques del transmisor de la Figura 6 y al diagrama de flujo lógico de la Figura 8, se utiliza un registro de cuenta de secuencia 150 para proporcionar una cuenta de secuencia de transmisión, que se incrementa con cada nuevo evento de transmisión (identificado por el mensaje en el que al menos un bit en el registro de estado 152 ha cambiado desde la transmisión anterior). De este modo, la lógica asociada con el registro de estado 152 incrementará el contador de secuencia 150 cuando cualquier bit haya cambiado. El preámbulo 92, los bits de estado 96, el número de identificación (número de serie) 94 y el CRC 98 se ensamblan junto con la cuenta de secuencia 100 y la cuenta de secuencia inversa 102 en el mensaje de dos partes que se procesa por el codificador de RZ 104 y el codificador de NRZ 106 según se describió anteriormente. De este modo, incrementando el contador de secuencia 150 siempre que se ha cambiado un bit de estado, el panel de control puede determinar si un mensaje se ha recibido fuera de secuencia desde un transmisor dado, según aquí se describe.

Después de codificar la primera parte de mensaje en el formato de RZ y la segunda parte de mensaje (la información de secuencia) en el formato NRZ, se transmite el mensaje. Por supuesto, cada dispositivo de seguridad/transmisor en el sistema, probablemente tendrá diferentes cuentas de secuencias en cualquier momento dado, puesto que cada uno opera de forma asíncrona entre sí. Según se describe a continuación, el dispositivo receptor (panel de control) efectuará un seguimiento de registro de la cuenta de secuencia para cada transmisor, de forma individual, para determinar el secuenciamiento adecuado para cada transmisor.

Según se ilustra en las Figuras 7 y 9, el dispositivo receptor recibe y demodula el mensaje inalámbrico y luego, procede a decodificar el mensaje con el decodificador de RZ 114 y el decodificador de NRZ 112 según se describió anteriormente. Los circuitos de análisis de datos y la lógica procesan, entonces, el mensaje mediante la extracción, en primer lugar, de la cuenta de secuencia 126 y de la cuenta de secuencia inversa 128 y del número de identificación del transmisor desde el mensaje. Una cuenta de secuencia anterior, asociada con el número de identificación del transmisor, se recupera desde una tabla de cuentas de secuencias 134 en la memoria. La cuenta de secuencia 126, desde el mensaje, se compara con la cuenta de secuencia anterior recuperada desde la tabla. Si la cuenta de secuencia desde el mensaje es menor o igual a la cuenta de secuencia anterior, entonces, el dispositivo receptor ignora el mensaje y no toma ninguna nueva acción. Si, sin embargo, la cuenta de secuencia desde el mensaje no es menor que la cuenta de secuencia anterior, entonces, el dispositivo receptor procesa el mensaje (esto es, la parte de estado) y sustituye la cuenta de secuencia anterior, en la tabla, con la cuenta de secuencia desde el mensaje. Como con la primera forma de realización anteriormente descrita, la cuenta de secuencia inversa 128 se utiliza también, si así se desea, como un control de la integridad de datos.

En consecuencia, si se recibe un mensaje "tardío", lo que significa que contiene información desfasada que induciría a error al panel de control, en tal caso se ignorará. Según se describió anteriormente, esto puede suceder, a modo de ejemplo, si se abre una puerta y luego, se cierra con rapidez, de modo que se envíe un grupo de mensajes de "puerta abierta" por un transmisor y luego, un grupo de mensajes de "puerta cerrada" se envía por el transmisor inmediatamente después. (Conviene señalar que los mensajes se suelen enviar en grupos de mensajes tal como un sexteto, lo que mejora la fiabilidad y aumenta las posibilidades de una transmisión satisfactoria, como es bien conocido en esta técnica). Puesto que uno de los mensajes desde el grupo de "puerta abierta" puede llegar al panel de control después de uno de los mensajes desde el grupo de "puerta cerrada" debido a retrasos en el procesamiento por receptores distantes, bits eliminados, etc., el panel de control determinará, con esta invención, que la cuenta de secuencia desde el mensaje de "puerta abierta" es menor que el del mensaje "puerta cerrada" y en consecuencia, lo ignorará. Esta invención permite, de este modo, al panel de control determinar si un mensaje recibido desde un determinado transmisor puede estar fuera de secuencia debido a retrasos en la recepción, procesamiento, etc., por uno de los receptores en el sistema.

Conviene señalar que, en algún punto, la cuenta de secuencia debe reponerse a cero. En la forma de realización preferida que utiliza una cuenta de secuencia de ocho bits, la secuencia de cuentas será 0, 1, 2, 3, 4, 5, 6, 7, …254, 255, 0, 1, 2, 3, 4, etc. La lógica de procesamiento está programada para reconocer que una cuenta de 0 se considera mayor que una cuenta de 255, de modo que cuando se detecta 0 después de 255, el control no considerará, de forma errónea, como que es una transmisión fuera de secuencia.

Conviene señalar, además, que la forma de realización preferida se dará a conocer para el borrador de los datos de cuenta de secuencia desde la tabla sobre una base periódica, a modo de ejemplo, cada minuto. Después de que se borren los datos de la cuenta de secuencia, entonces la nueva cuenta de secuencia recibida desde una transmisión de datos será memorizada y utilizada según se describió anteriormente. Esta circunstancia operativa eliminará la información desfasada y ayudará a resincronizar las cuentas de secuencia si fuera necesario, a modo de ejemplo, si un dispositivo transmisor es sustituido y debe sincronizarse la cuenta de secuencia.

REIVINDICACIONES

1. Un método de transmisión de un mensaje desde un dispositivo de seguridad (4, 6, 8) hacia un dispositivo receptor (10) que comprende las etapas siguientes:

a. formar un mensaje de datos en dos partes (28) que comprende una primera parte de mensaje y una segunda parte de mensaje,

i. la primera parte del mensaje que comprende

1. una parte de preámbulo (30)

2. una parte de número de identificación (32) que identifica, de manera única, el dispositivo de seguridad,

3. una parte de estado (34) que comprende datos de estado indicativos del estado del dispositivo de seguridad y

4. una parte de CRC (36) que contiene datos CRC basados en una función CRC ejecutada en la parte de número de identificación y la parte de estado y

ii. la segunda parte del mensaje que comprende:

1. una primera parte de estado redundante (38) que comprende los datos de estado (34) procedentes de la primera parte del mensaje y

2. una segunda parte de estado redundante (40) que comprende los datos de estado (34) procedentes de la primera parte de mensaje, en donde la segunda parte de estado redundante (40) es la inversa lógica de la primera parte de estado redundante de la segunda parte de mensaje;

b. codificar la primera parte de mensaje en un primer formato de codificación;

c. codificar la segunda parte de mensaje en un segundo formato de codificación diferente del primer formato de codificación;

d. modular una señal portadora con la primera parte de mensaje codificada y la segunda parte de mensaje codificada y

e. transmitir la señal portadora modulada.

2. El método según la reivindicación 1, en donde el primer formato de codificación es un formato de reposición a cero, RZ.

3. El método según la reivindicación 2, en donde el formato RZ es el formato de Manchester.

4. El método según la reivindicación 2, en donde el segundo formato de codificación es un formato sin reposición a cero, NRZ.

5. El método según la reivindicación 1, en donde el segundo formato de codificación es un formato de reposición a cero, RZ.

6. El método según la reivindicación 5, en donde el formato RZ es el formato de Manchester.

7. El método según la reivindicación 5, en donde el primer formato de codificación es un formato sin reposición a cero, NZR.

8. Un método de explotación de un sistema de seguridad (2) que comprende las etapas siguientes:

a. la realización, en un transmisor (4, 6, 8), las etapas del método según la reivindicación 1 y

b. la recepción, en un dispositivo receptor (10), de la señal portadora modulada;

c. la demodulación de la señal portadora modulada recibida;

d. la decodificación de la primera parte de mensaje utilizando el primer formato de codificación para obtener la parte de preámbulo (30), la parte de número de identificación (32), la parte de estado (34) y la parte de CRC (36);

e. la decodificación de la segunda parte de mensaje utilizando el segundo formato de codificación para obtener la primera parte de estado redundante (38) y la segunda parte de estado redundante (40) y

f. analizar dos partes, o más, entre

i. la parte de estado (34),

ii. la primera parte de estado redundante (38),

iii. la segunda parte de estado redundante (40) y

iv. la parte de CRC (36),

con el fin de determinar si el mensaje (28) fue recibido de manera válida.

9. El método según la reivindicación 8 en donde, si la etapa que comprende analizar dos partes, o más, entre la parte de estado, la primera parte de estado redundante, la segunda parte de estado redundante y la parte de CRC, de manera que se determine si el mensaje fue recibido de manera válida, indica que el mensaje ha sido válidamente recibido y entonces, el mensaje se señala como habiendo sido válidamente recibido.

10. El método según la reivindicación 8 en donde, si la etapa que comprende analizar dos partes, o más, entre la parte de estado, la primera parte de estado redundante, la segunda parte de estado redundante y la parte de CRC con el fin de determinar si el mensaje fue recibido de manera válida, lo que indica que el mensaje no ha sido recibido de manera válida, entonces el mensaje es etiquetado como no habiendo sido recibido de manera válida.

11. El método según la reivindicación 8 en donde la etapa de analizar dos o más de entre la parte de estado, la primera parte de estado redundante, la segunda parte de estado redundante y la parte de CRC con el fin de determinar si el mensaje fue recibido de manera válida, comprende las etapas siguientes:

1. comparar la parte de estado con la primera parte de estado redundante;

2. si la parte de estado es la misma que la primera parte de estado redundante, etiquetar el mensaje como habiendo sido recibido de manera válida.

12. El método según la reivindicación 8 en donde la etapa que comprende analizar dos partes, o más, entre la parte de estado, la primera parte de estado redundante, la segunda parte de estado redundante y la parte de CRC de manera que se determine si el mensaje ha sido recibido de manera válida comprende las etapas siguientes:

1. comparar la parte de estado con la segunda parte de estado redundante;

2. si la parte de estado es la misma que la segunda parte de estado redundante, en tal caso, etiquetar el mensaje como habiendo sido recibido de manera válida.

13. El método según la reivindicación 8, en donde la etapa que comprende analizar dos partes, o más, entre la parte de estado, la primera parte de estado redundante, la segunda parte de estado redundante y la parte de CRC de manera que se determine si el mensaje fue recibido de manera válida, comprende las etapas siguientes:

1. comparar la parte de estado con la primera parte de estado redundante y con la segunda parte de estado redundante;

2. si la parte de estado, la primera parte de estado redundante y la segunda parte de estado redundante son todas ellas las mismas, en tal caso, etiquetar el mensaje como habiendo sido recibido de manera válida.

14. El método según la reivindicación 8, en donde la etapa que comprende analizar dos partes, o más, entre la parte de estado, la primera parte de estado redundante, la segunda parte de estado redundante y la parte de CRC de manera que se determine si el mensaje fue recibido de manera válida, comprende las etapas siguientes:

1. generar un CRC basado en la parte de número de identificación y la parte de estado;

2. comparar el CRC generado con la parte de CRC del mensaje;

3. si el CRC generado es el mismo que la parte de CRC del mensaje, en tal caso etiquetar el mensaje como habiendo sido recibido de manera válida;

4. si el CRC generado no es el mismo que la parte de CRC del mensaje, entonces:

a. comparar la parte de estado con la primera parte de estado redundante y con la segunda parte de estado redundante;

b. si la parte de estado, la primera parte de estado redundante y la segunda parte de estado redundante son todas ellas las mismas, en tal caso etiquetar el mensaje como habiendo sido recibido de manera válida.

15. El método según la reivindicación 8 en donde la etapa que comprende analizar dos partes, o más, entre la parte de estado, la primera parte de estado redundante, la segunda parte de estado redundante y la parte de CRC de manera que se determine si el mensaje fue recibido de manera válida, comprende las etapas siguientes:

1. comparar la primera parte de estado redundante y la segunda parte de estado redundante;

2. si la primera parte de estado redundante y la segunda parte de estado redundante son las mismas, entonces:

a. comparar una u otra de la primera parte de estado redundante y de la segunda parte de estado redundante con la parte de estado y

b. etiquetar el mensaje como habiendo sido recibido de manera válida cuando la comparación se realiza positivamente.

16. El método según la reivindicación 8 en donde la etapa que comprende analizar dos partes, o más, entre la parte de estado, la primera parte de estado redundante, la segunda parte de estado redundante y la parte de CRC de manera que se determine si el mensaje fue recibido de manera válida, comprende las etapas siguientes:

1. generar un CRC basado en la parte de número de identificación y la parte de estado;

2. comparar el CRC generado con la parte de CRC del mensaje;

3. si el CRC generado es el mismo que la parte de CRC del mensaje, entonces:

a. comparar la primera parte de estado redundante y la segunda parte de estado redundante;

b. si la primera parte de estado redundante es la misma que la segunda parte de estado redundante, etiquetar el mensaje como habiendo sido recibido de manera válida y

4. si el CRC generado no es el mismo que la parte de CRC del mensaje, entonces.

a. comparar la primera parte de estado redundante con la segunda parte de estado redundante;

b. si la primera parte de estado redundante es la misma que la segunda parte de estado redundante, entonces:

i. generar un segundo CRC basado en el número de identificación y en la primera parte de estado redundante;

ii. comparar el segundo CRC generado con la parte de CRC del mensaje;

iii. si la comparación es realizada positivamente, utilizar la primera parte de estado redundante como parte de estado redundante recibida de manera válida y

iv. si la comparación proporciona un resultado negativo, etiquetar el mensaje como no habiendo sido recibido de manera válida.

17. Un dispositivo de seguridad destinado a utilizarse en un sistema de seguridad, cuyo dispositivo de seguridad comprende un transmisor diseñado para realizar las etapas de transmisor según la reivindicación 1.

18. Un sistema de seguridad que comprende:

a. un dispositivo de seguridad según se reivindica en la reivindicación 17 y

b. un dispositivo de recepción adaptado para realizar las etapas del dispositivo de recepción según una cualquiera de las reivindicaciones 8 a 16.

19. Un método de transmisión de un mensaje desde un dispositivo de seguridad (4, 6, 8) hacia un dispositivo receptor (10) que comprende las etapas siguientes:

a. formar un mensaje de datos en dos partes (90) que comprende una primera parte de mensaje y una segunda parte de mensaje,

i. la primera parte de mensaje comprendiendo

1. una parte de preámbulo (92),

2. una parte de número de identificación (94) que identifica, de manera única, el dispositivo de seguridad,

3. una parte de estado (96) que comprende datos de estado indicativos del estado del dispositivo de seguridad (4, 6, 8) y

4. una parte de CRC (98) que contiene datos CRC basados en una función CRC ejecutada en la parte de número de identificación y la parte de estado (96) y

ii. la segunda parte de mensaje que comprende una cuenta de secuencia (100) que es indicativa del secuenciamiento relativo de los mensajes procedentes del dispositivo de seguridad;

b. codificar la primera parte de mensaje en un primer formato de codificación;

c. codificar la segunda parte de mensaje en un segundo formato de codificación diferente del primer formato de codificación;

d. modular una señal portadora con la primera parte de mensaje codificada y la segunda parte de mensaje codificada y

e. transmitir la señal portadora modulada.

20. El método según la reivindicación 19 en donde el primer formato de codificación es un formato de reposición a cero, RZ.

21. El método según la reivindicación 20, en donde el formato RZ es el formato denominado Manchester.

22. El método según la reivindicación 20, en donde el segundo formato de codificación es un formato sin reposición a cero, NRZ.

23. El método según la reivindicación 19, en donde el segundo formato de codificación es un formato de reposición a cero, RZ.

24. El método según la reivindicación 23, en donde el formato RZ es el formato denominado Manchester.

25. El método según la reivindicación 23, en donde el primer formato de codificación es un formato sin reposición a cero, NRZ.

26. El método según la reivindicación 19 que comprende, además, las etapas siguientes:

determinar si cualesquiera bits de los bits de estado en la parte de estado (96) de la primera parte de mensaje del mensaje han cambiado con respecto a un mensaje previamente transmitido;

si cualesquiera bits de los bits de estado han cambiado, entonces incrementar la cuenta de secuencia (100) del mensaje previamente transmitido y

si no ha cambiado ningún bit de los bits de estado, entonces utilizar la misma cuenta de secuencia (100) que en el mensaje previamente transmitido.

27. Un método de explotación de un sistema de seguridad que comprende las etapas siguientes:

a. realizar, en un transmisor (4, 6, 8), las etapas del método según la reivindicación 19;

b. recibir, en el dispositivo receptor (10), la señal portadora modulada;

c. demodular la señal portadora modulada recibida;

d. decodificar la primera parte de mensaje utilizando el primer formato de codificación para obtener la parte de preámbulo, la parte de número de identificación, la parte de estado y la parte de CRC;

e. decodificar la segunda parte de mensaje utilizando el segundo formato de codificación para obtener la cuenta de secuencia y

f. procesar el mensaje según las etapas siguientes:

i. recuperar, desde memoria, una cuenta de secuencia precedente asociada con el número de identificación;

ii. comparar la cuenta de secuencia del mensaje con la cuenta de secuencia precedente que procede de la memoria;

1. si la cuenta de secuencia del mensaje es inferior o igual a la cuenta de secuencia precedente, ignorar el mensaje y

2. si la cuenta de secuencia del mensaje no es inferior o igual a la cuenta de secuencia precedente, entonces procesar el mensaje y sustituir la cuenta de secuencia precedente, que procede de la memoria por la cuenta de secuencia procedente del mensaje.

28. El método según la reivindicación 27, que comprende, además, las etapas siguientes:

determinar si cualquiera de los bits de estado de la parte de estado de la primera parte de mensaje del mensaje han cambiado con respecto a un mensaje previamente transmitido;

si cualesquiera bits de los bits de estado han cambiado, entonces incrementar la cuenta de secuencia del mensaje previamente transmitido y

si no ha cambiado ningún bit de los bits de estado, entonces utilizar la misma cuenta de secuencia que en el mensaje previamente transmitido.

29. Un dispositivo de seguridad (4, 6, 8) para su uso en un sistema de seguridad (2) que comprende un transmisor adaptado para realizar las etapas del transmisor según la reivindicación 27 o 28.

30. Un sistema de seguridad (2) que comprende:

a. un dispositivo de seguridad (4, 6, 8) tal como se reivindica en la reivindicación 29 y

b. un dispositivo receptor (10) adaptado para realizar las etapas del método del dispositivo de recepción de la reivindicación 27 o 28.

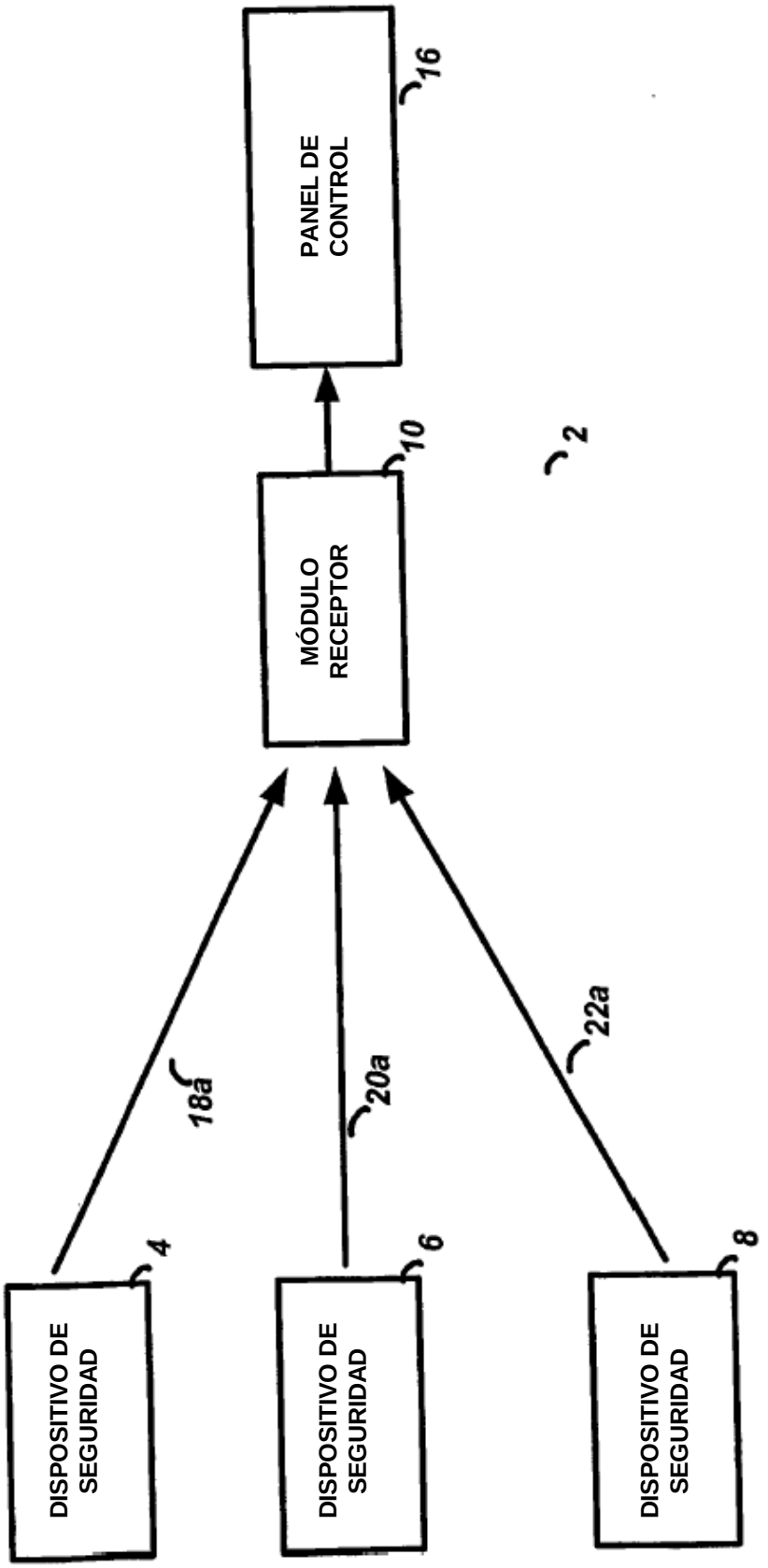
PANEL DE CONTROL
16
MÓDULO RECEPTOR
10
2
18a
20a
22a
DISPOSITIVO DE SEGURIDAD
4
DISPOSITIVO DE SEGURIDAD
6
DISPOSITIVO DE SEGURIDAD
8

Figura 1

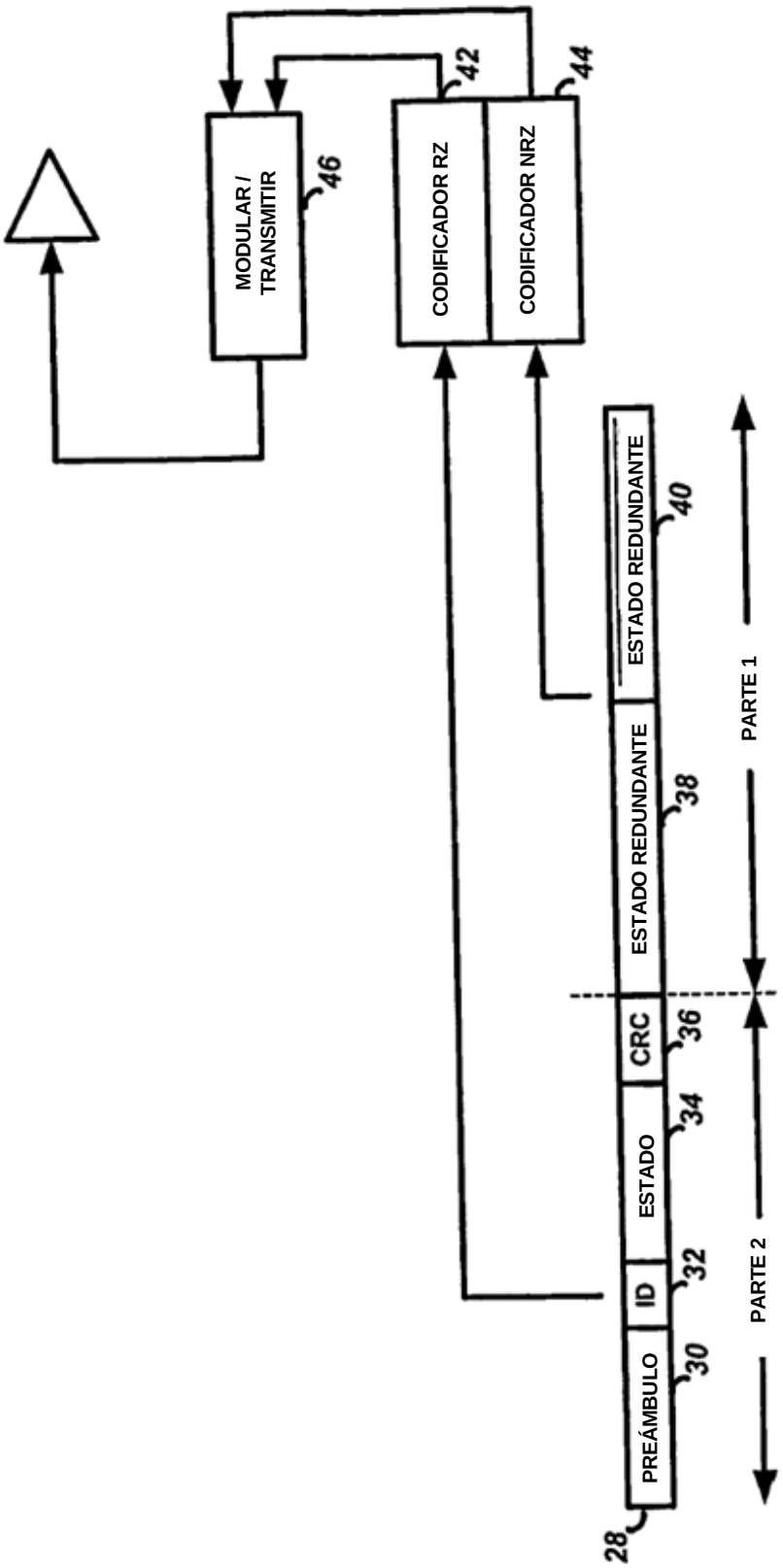
MODULAR / TRANSMITIR
46
CODIFICADOR RZ
42
CODIFICADOR NRZ
44
ESTADO REDUNDANTE
40
ESTADO REDUNDANTE
38
CRC
36
ESTADO
34
ID
32
PREÁMBULO
30
28
PARTE 1
PARTE 2

Figura 2

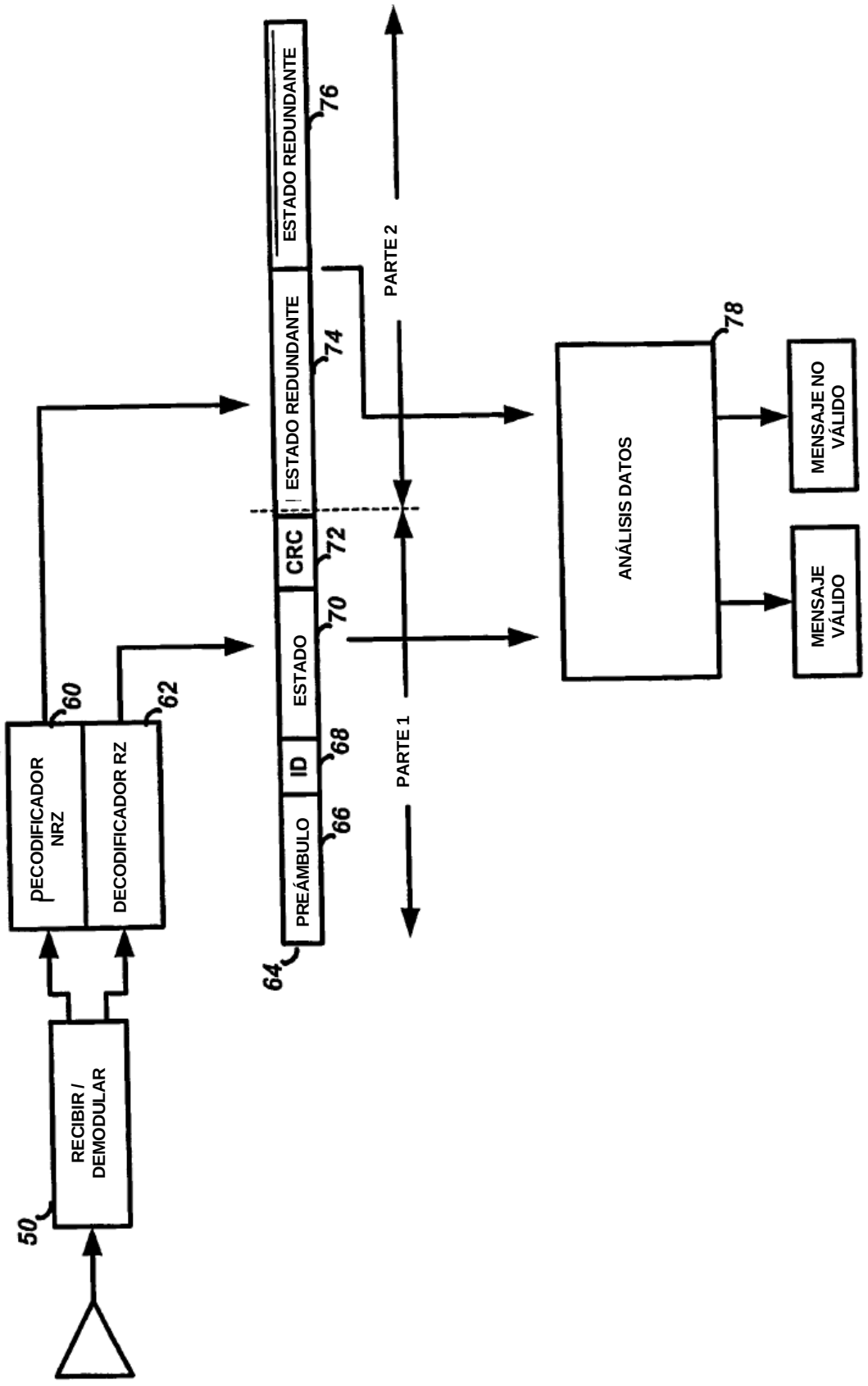
RECIBIR / DEMODULAR
50
DECODIFICADOR NRZ
DECODIFICADOR RZ
60
62
PREÁMBULO
ID
ESTADO
CRC
ESTADO REDUNDANTE
ESTADO REDUNDANTE
64
66
68
70
72
74
76
PARTE 1
PARTE 2
ANÁLISIS DATOS
78
MENSAJE NO VÁLIDO
MENSAJE VÁLIDO

Figura 3

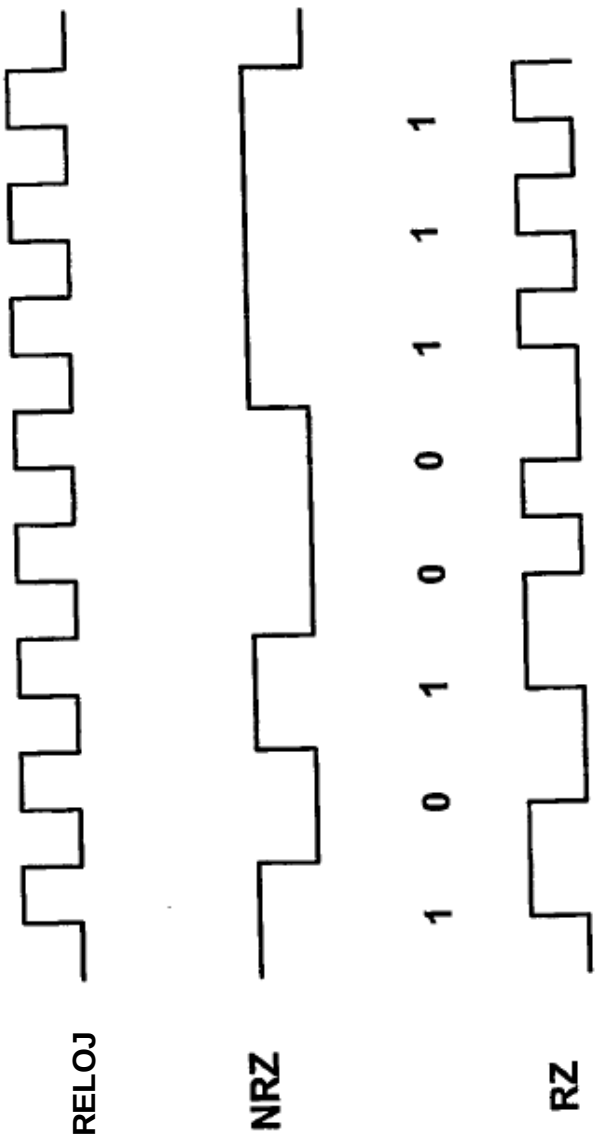

Figura 4

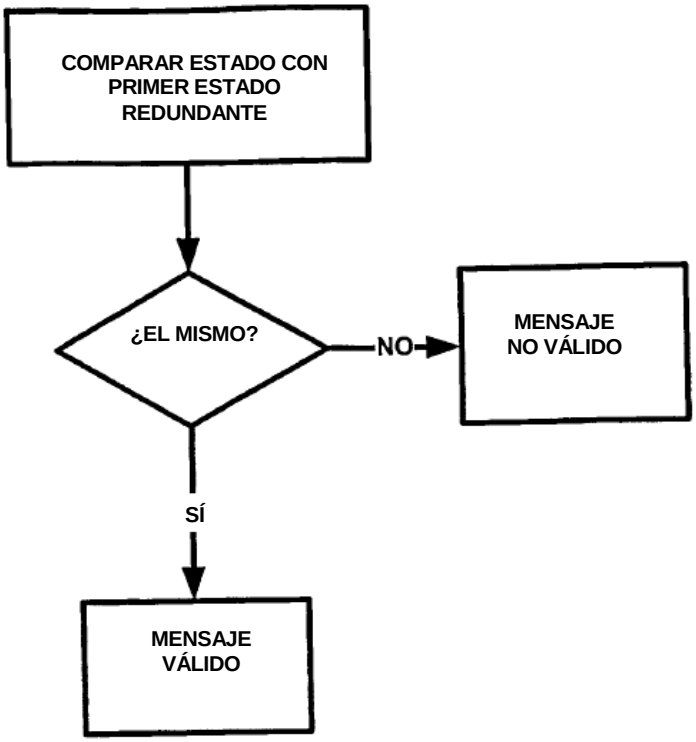

Figura 5A

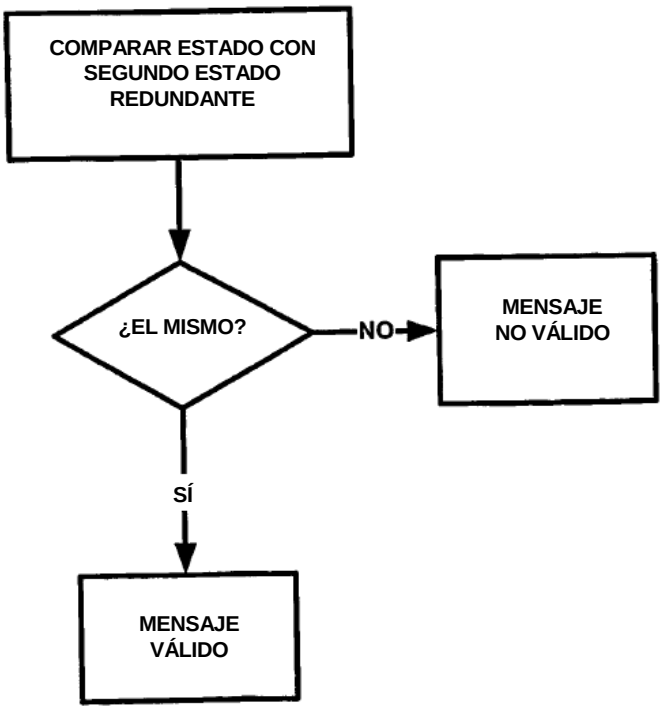

Figura 5B

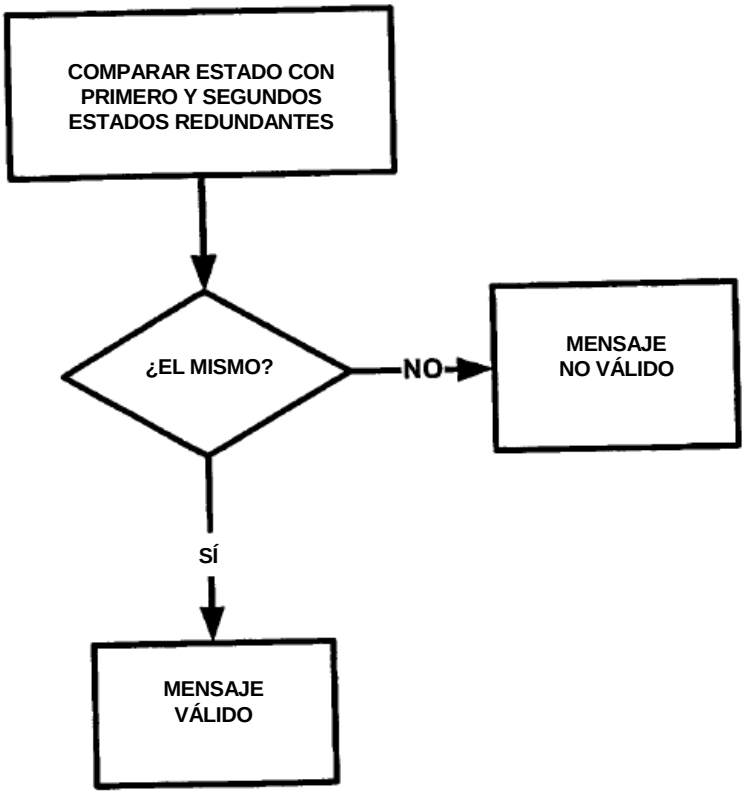
COMPARAR ESTADO CON PRIMERO Y SEGUNDOS ESTADOS REDUNDANTES
¿EL MISMO?
NO
MENSAJE NO VÁLIDO
SÍ
MENSAJE VÁLIDO

Figura 5C

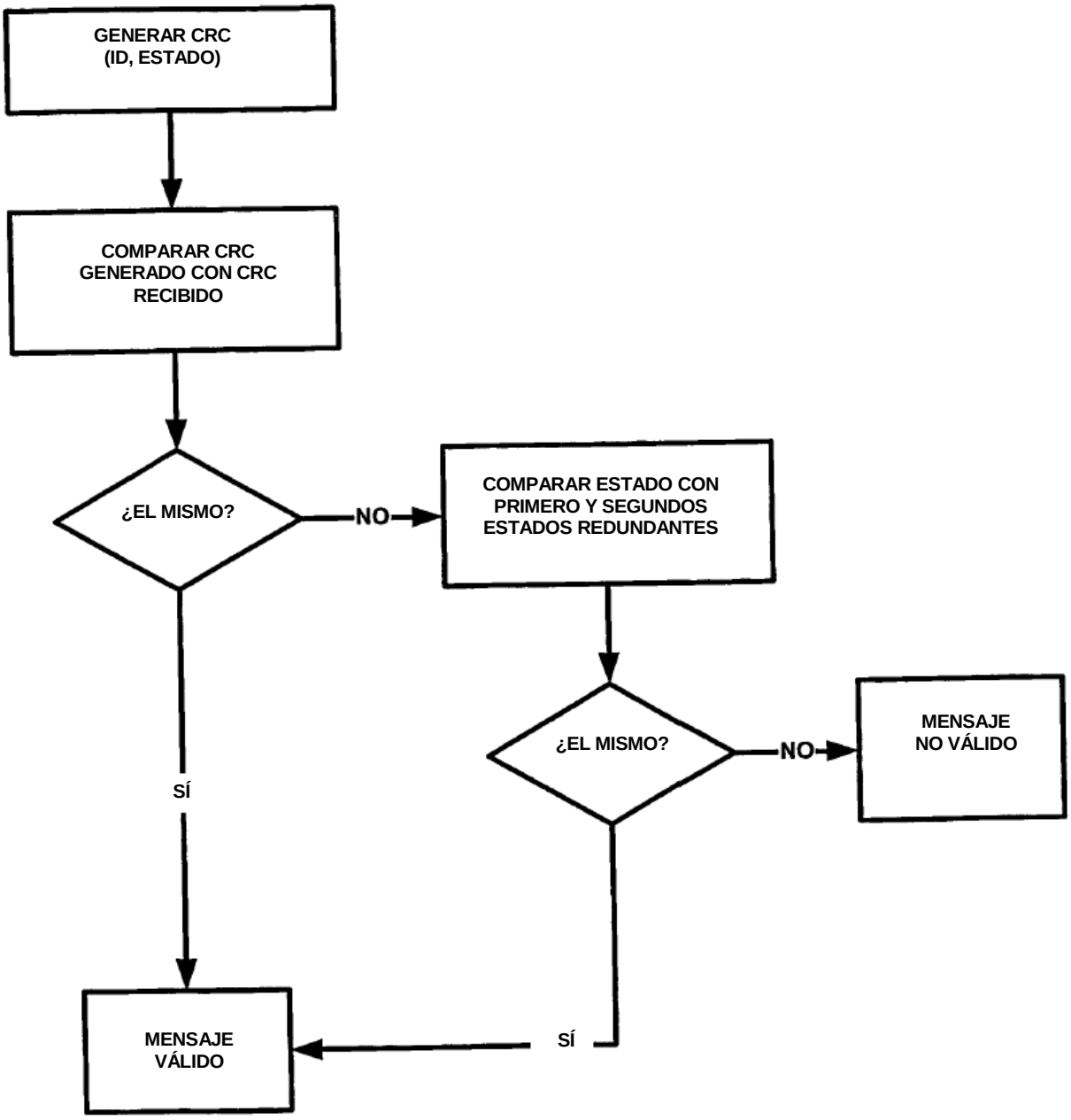
GENERAR CRC
(ID, ESTADO)
COMPARAR CRC
GENERADO CON CRC
RECIBIDO
¿EL MISMO?
NO
COMPARAR ESTADO CON
PRIMERO Y SEGUNDOS
ESTADOS REDUNDANTES
SÍ
¿EL MISMO?
NO
MENSAJE
NO VÁLIDO
MENSAJE
VÁLIDO
SÍ

Figura 5D

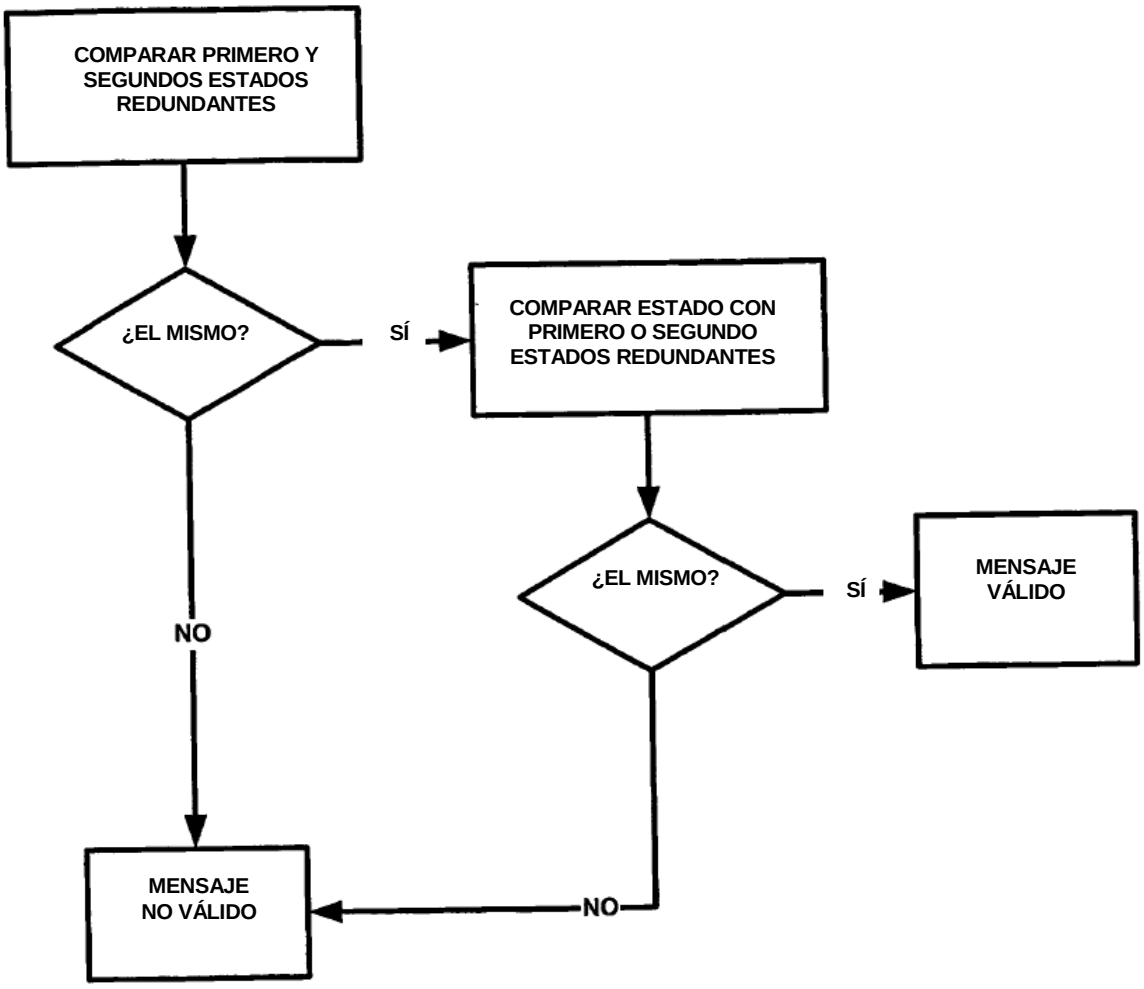
COMPARAR PRIMERO Y SEGUNDOS ESTADOS REDUNDANTES
¿EL MISMO?
SÍ
COMPARAR ESTADO CON PRIMERO O SEGUNDO ESTADOS REDUNDANTES
¿EL MISMO?
SÍ
MENSAJE VÁLIDO
NO
MENSAJE NO VÁLIDO
NO

Figura 5E

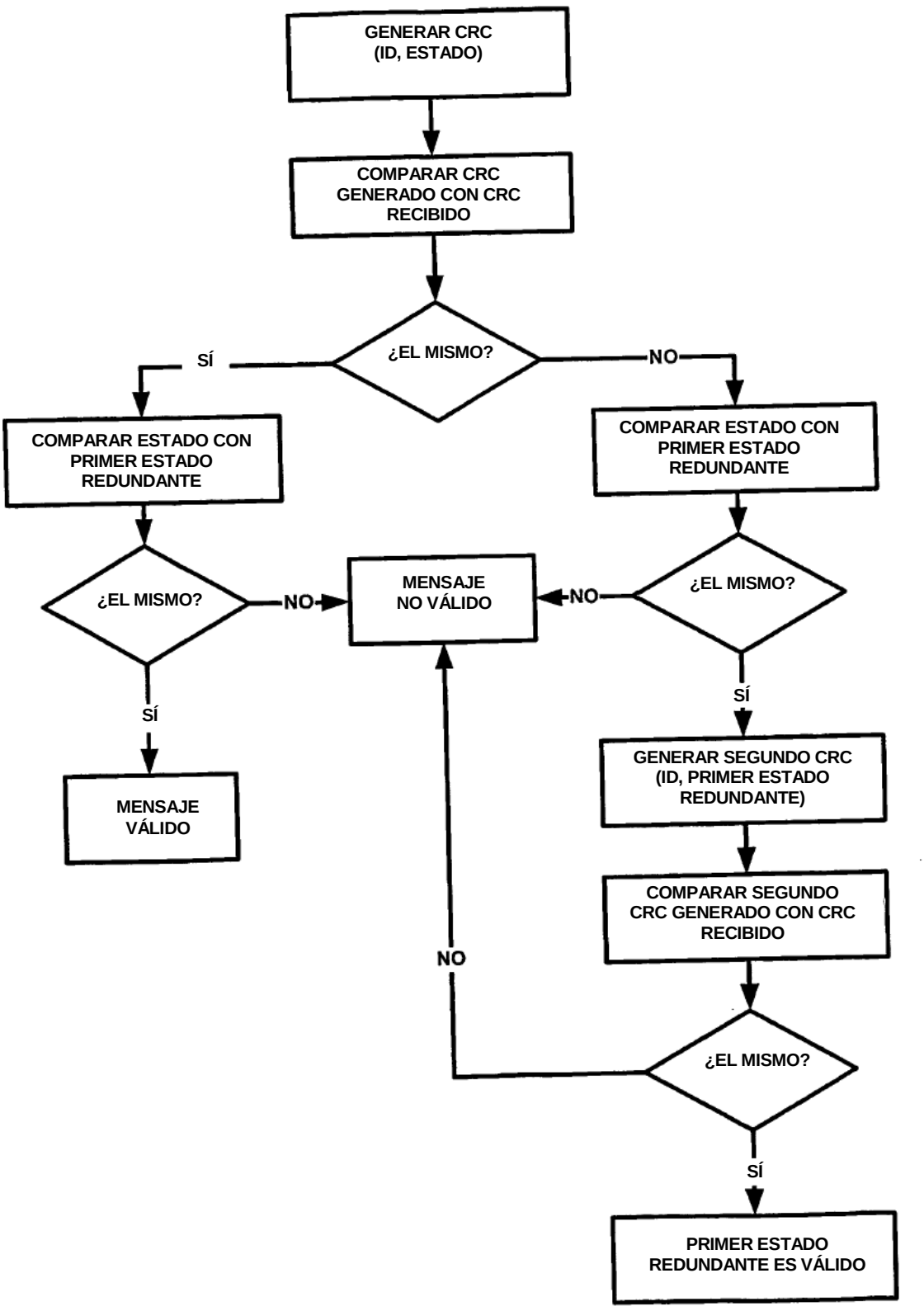
GENERAR CRC
(ID, ESTADO)
COMPARAR CRC
GENERADO CON CRC
RECIBIDO
¿EL MISMO?
SÍ
NO
COMPARAR ESTADO CON
PRIMER ESTADO
REDUNDANTE
COMPARAR ESTADO CON
PRIMER ESTADO
REDUNDANTE
¿EL MISMO?
NO
MENSAJE
NO VÁLIDO
NO
¿EL MISMO?
SÍ
MENSAJE
VÁLIDO
SÍ
GENERAR SEGUNDO CRC
(ID, PRIMER ESTADO
REDUNDANTE)
COMPARAR SEGUNDO
CRC GENERADO CON CRC
RECIBIDO
NO
¿EL MISMO?
SÍ
PRIMER ESTADO
REDUNDANTE ES VÁLIDO

Figura 5F

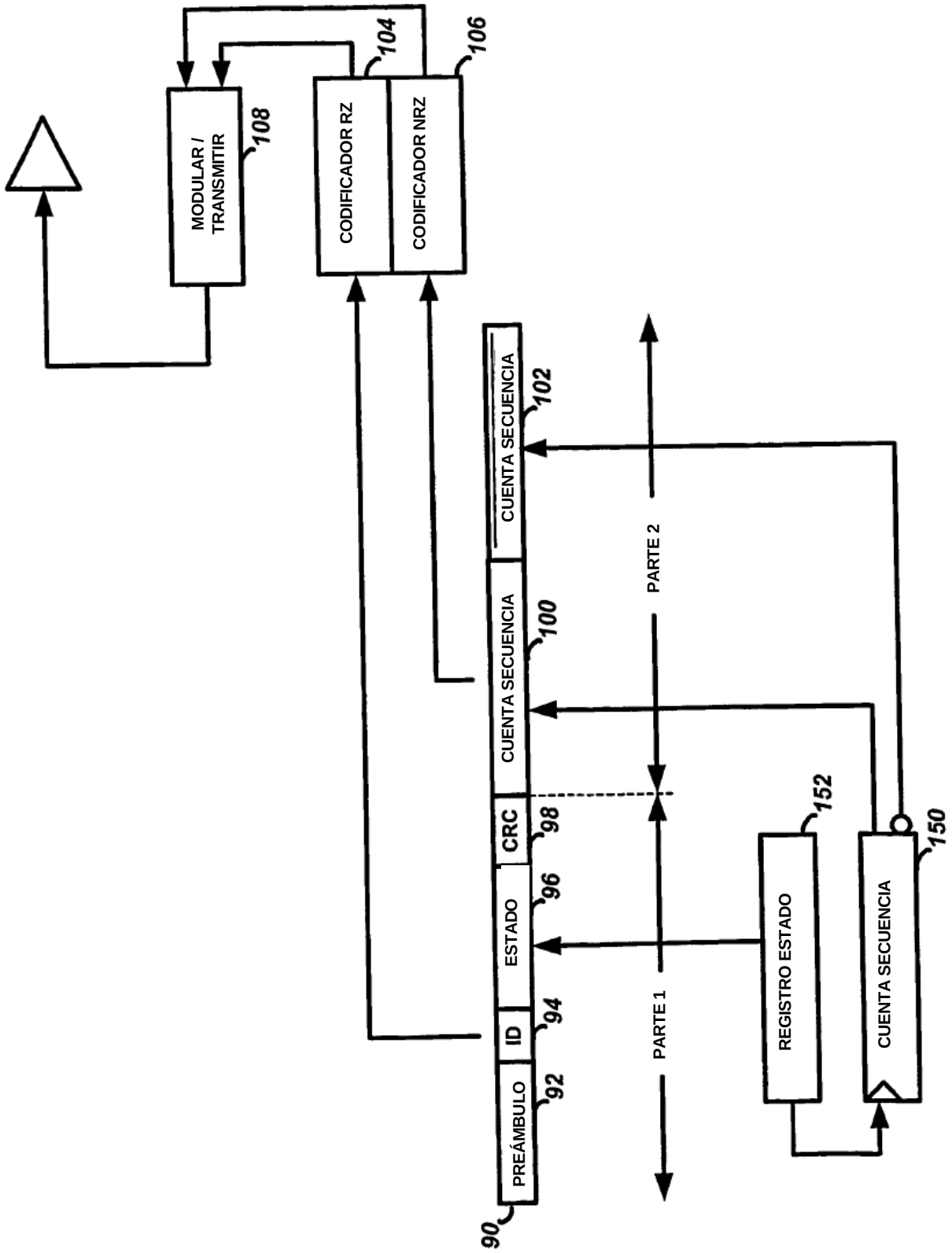
MODULAR / TRANSMITIR
108
CODIFICADOR RZ
104
CODIFICADOR NRZ
106
CUENTA SECUENCIA
102
CUENTA SECUENCIA
100
CRC
98
ESTADO
96
ID
94
PREÁMBULO
92
90
PARTE 2
PARTE 1
REGISTRO ESTADO
152
CUENTA SECUENCIA
150

Figura 6

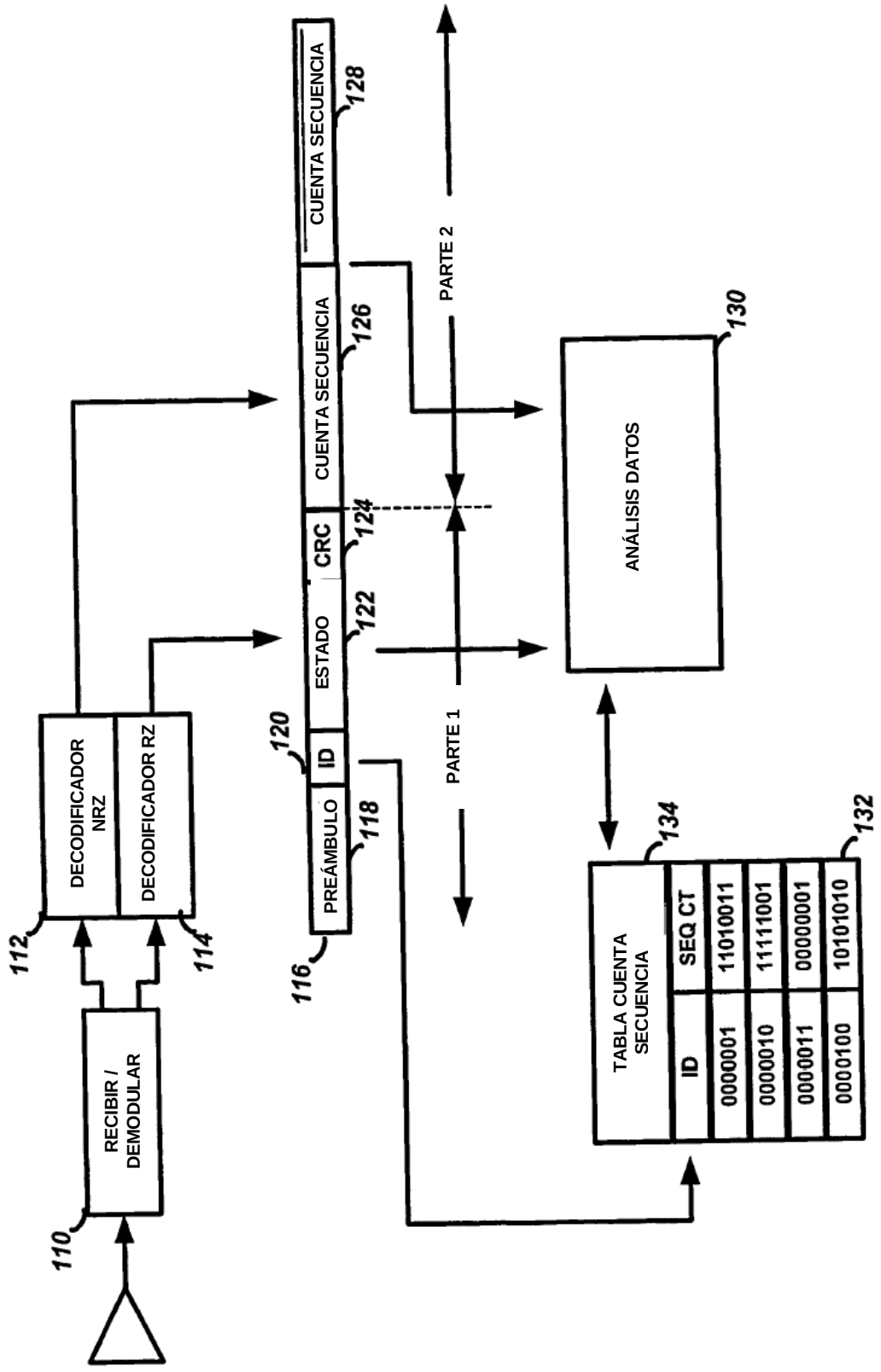
RECIBIR / DEMODULAR
110
DECODIFICADOR NRZ
DECODIFICADOR RZ
112
114
PREÁMBULO
ID
ESTADO
CRC
CUENTA SECUENCIA
CUENTA SECUENCIA
116
118
120
122
124
126
128
PARTE 1
PARTE 2
ANÁLISIS DATOS
130
TABLA CUENTA SECUENCIA
ID
SEQ CT
0000001
11010011
0000010
11111001
0000011
00000001
0000100
10101010
132
134

Figura 7

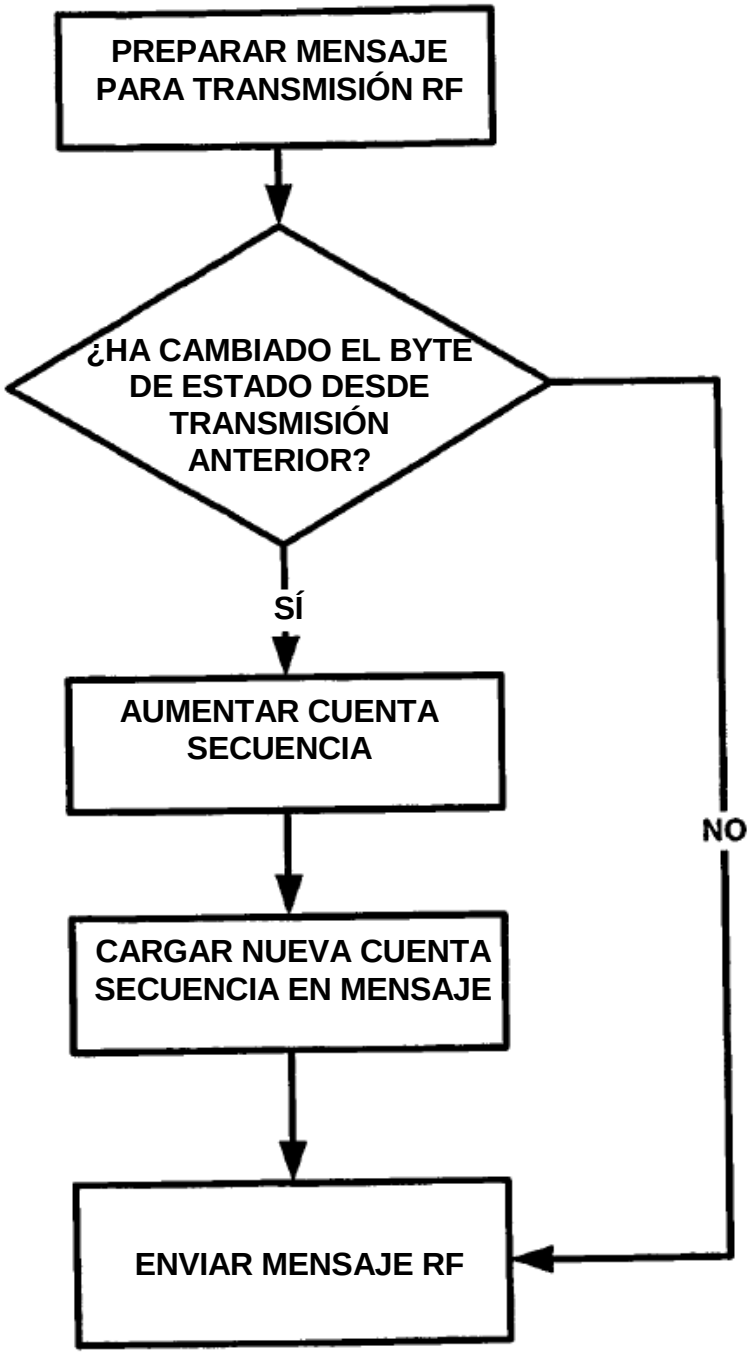
PREPARAR MENSAJE PARA TRANSMISIÓN RF
¿HA CAMBIADO EL BYTE DE ESTADO DESDE TRANSMISIÓN ANTERIOR?
SÍ
NO
AUMENTAR CUENTA SECUENCIA
CARGAR NUEVA CUENTA SECUENCIA EN MENSAJE
ENVIAR MENSAJE RF

Figura 8

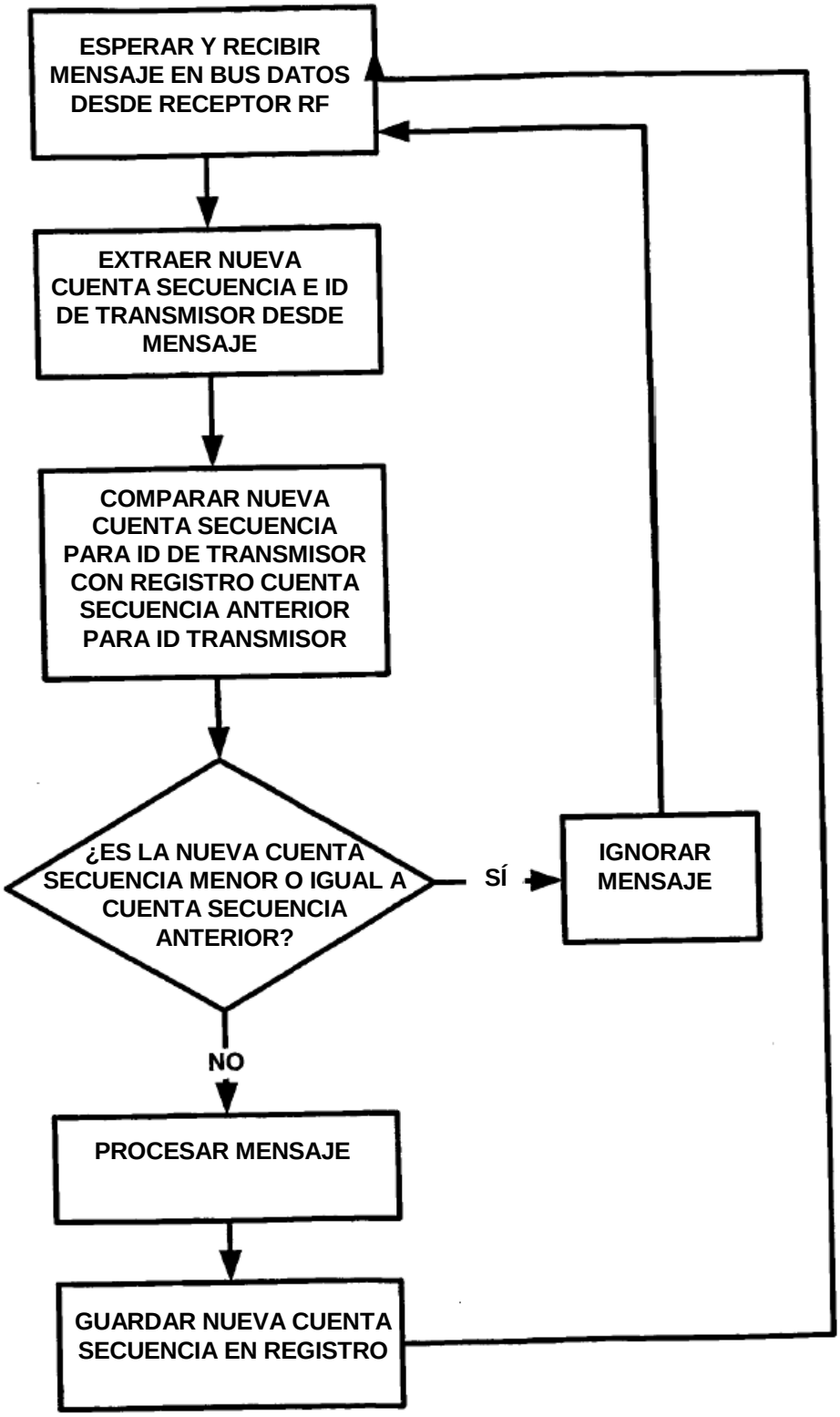
ESPERAR Y RECIBIR MENSAJE EN BUS DATOS DESDE RECEPTOR RF
EXTRAER NUEVA CUENTA SECUENCIA E ID DE TRANSMISOR DESDE MENSAJE
COMPARAR NUEVA CUENTA SECUENCIA PARA ID DE TRANSMISOR CON REGISTRO CUENTA SECUENCIA ANTERIOR PARA ID TRANSMISOR
¿ES LA NUEVA CUENTA SECUENCIA MENOR O IGUAL A CUENTA SECUENCIA ANTERIOR?
SÍ
IGNORAR MENSAJE
NO
PROCESAR MENSAJE
GUARDAR NUEVA CUENTA SECUENCIA EN REGISTRO

Figura 9