(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 485 366**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.07.2006 E 06116634 (4)**

(97) Fecha y número de publicación de la concesión europea: **11.06.2014 EP 1841165**

(54) Título: **Transmisión de información segura de a través de equipos de seguridad no aprobada**

(30) Prioridad:

28.03.2006 EP 06111844

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.08.2014

(73) Titular/es:

SAAB AB (100.0%)
581 88 Linköping , SE

(72) Inventor/es:

ERIKSSON, JAN-ERIK;
JOHANSSON, RIKARD y
STENDAHL, PETER

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Transmisión de información segura de a través de equipos de seguridad no aprobada

Campo de la invención

La presente invención se refiere a procedimientos y dispositivos dentro de los sistemas electrónicos para la transferencia de señales de información de una manera segura. En particular, se refiere a tales procedimientos y dispositivos para comunicar con seguridad un mensaje desde una entidad de seguridad aprobada a otra entidad de seguridad aprobada a través de una entidad de seguridad no aprobada.

Antecedentes

Cuando se desarrolla software de equipo de sistemas transportados por aire, es común practicar un estándar conocido como RTCA/DO - 178B. El estándar requiere que los sistemas sean clasificados en lo que se refiere a su nivel de criticidad. El estándar requiere que un sistema que puede causar o contribuir a un mal funcionamiento de un cierto grado de gravedad debe ser desarrollado de acuerdo con ciertas reglas. El software se clasifica en 5 niveles, de A a E, en el que A corresponde al nivel más crítico, y E al nivel menos crítico. El coste para desarrollar el software de clase A y B es de aproximadamente tres veces el costa para desarrollar el software de clase D. No existen requisitos en el estándar RTCA/DO - 178B en lo que se refiere al software de clase E, por lo que es difícil comparar los costes. El software debe ser desarrollado de acuerdo con la clase A si un error de software puede dar lugar a un accidente con víctimas, a la clase B, si el error puede conducir a lesiones personales extensas o niveles de seguridad gravemente reducidos y los niveles adicionales C, D, E corresponden a efectos menos severos de un error.

En muchas aplicaciones, una información errónea puede conducir a consecuencias muy graves (en estas aplicaciones, el software de clase A sería el aplicable). Como ejemplo, se puede considerar un caso en el que se envía una información errónea a un sistema de armas, que conduce a un bombardeo erróneo.

El software clasificada como de tipo A o B es caro de desarrollar y, en principio, no se permite que se integre o ejecute en un ordenador comercial utilizando el software comercial disponible en el mercado (software COTS) tal como el sistema operativo Windows o Linux. Tradicionalmente, por lo tanto, todos los sistemas dentro de una cadena de información, han sido desarrollados como de clase A o B para el tipo de funciones que se ha mencionado más arriba.

En relación con la introducción de Vehículos Aéreos No Tripulados (UAV) existe la necesidad de controlar con seguridad estos vehículos utilizando principalmente productos COTS. Esto no es una alternativa si el procedimiento tradicional, véase más arriba, se debe usar para lograr una circulación segura de información. También en otras aplicaciones, el procedimiento tradicional resulta en mayores costos económicos que lo que sería el caso si los productos tuviesen una clase inferior de criticidad que A o B, o lo que sería el caso si los productos COTS pudiesen ser utilizados tanto para el hardware como para el software.

Una aplicación típica de la invención es hacer posible controlar de forma remota un UAV utilizando (en parte) productos de software e informáticos COTS de bajo costo, al mismo tiempo que se cumplen los requisitos de los estándares de seguridad aplicables, tales como RTCA/DO - 178B.

Un objeto de la presente invención es proporcionar un procedimiento para la comunicación en los sistemas críticos de seguridad sin tener que utilizar el equipo de seguridad aprobado en toda la cadena de comunicación, al mismo tiempo que todavía se pueden cumplir los estándares de seguridad aplicables, tales como RTCA/DO - 178B.

El documento US 20031130770 A1describe un procedimiento para asumir y mantener el control remoto seguro de una aeronave en caso de un ataque, o de incapacidad del piloto de la aeronave. El procedimiento incluye las etapas de proporcionar un enlace de transmisión seguro por y entre el primer medio de transmisión y el medio de recepción en una aeronave que debe ser controlada y el segundo medio de transmisión y de recepción en una ubicación alejada de la aeronave, y transmitir un comando para interrumpir el control de piloto e iniciar el control remoto de la aeronave. El procedimiento incluye el uso de cifrado y descifrado con la ayuda de clave o claves de cifrado.

El documento US 2004/216031 A1 desvela un procedimiento para identificar si la información en un documento original ha sido alterada en una copia del mismo. El procedimiento incluye las etapas de encriptación de la información pertinente y la reducción a una marca de versificación de un tipo que se añade al documento original. Una parte de verificación recibe una copia del documento, junto con la marca de versificación. La marca de versificación es descifrada y se compara con la información contenida en la copia. Una discrepancia indica que la copia podría haber sido alterada.

Sumario de la invención

El objeto anterior se resuelve por un procedimiento de comunicaciones de acuerdo con la reivindicación 1.

Un procedimiento de comunicación comprende las siguientes etapas:

En una primera entidad, transferir un primer conjunto de datos a un segundo conjunto de datos que representa la información en el primer conjunto de datos como una serie de segmentos gráficos. Estos segmentos pueden ser píxeles (representados por coordenadas x, y), líneas (representadas por dos conjuntos de coordenadas x / y que definen el inicio y el punto final de la línea), polígonos (definidos por una serie de coordenadas x / y que definen los ángulos de los polígonos) o cualquier otra forma de segmentos gráficos.

Transmitir el segundo conjunto de datos a través de una tercera entidad

Recibir el segundo conjunto de datos en una segunda entidad

Exhibir los segmentos gráficos definidos por el segundo conjunto de datos en la segunda entidad.

Determinar si el segundo de datos ha sido corrompido por la segunda o tercera entidad.

Tomar las medidas apropiadas dependiendo del resultado de lo anterior.

Las acciones apropiadas pueden ser ya sea para confiar y utilizar la información si parece que no han sido corrompida por la segunda o tercera entidad o tomar medidas que garanticen que la primera entidad conocerá que la información ya no puede ser recibida de una manera segura. Esto se puede lograr por la interrupción de una comunicación continua entre las entidades primera y segunda. Esta comunicación se puede implementar utilizando las siguientes etapas:

- Continuamente, desde la primera entidad, enviando un código único.
- Continuamente, en la segunda entidad, calculando un valor de retorno basado en algún algoritmo.
- Continuamente, en la primera entidad, verificando que el valor de retorno calculado desde la primera entidad es el correcto. Si no es así, la primera entidad debe tomar acciones apropiadas debido a la pérdida de comunicaciones con la segunda entidad.

Breve descripción de los dibujos

Estas y otras características, aspectos y ventajas de la presente invención se entenderán mejor con referencia a la descripción que sigue, reivindicaciones adjuntas, y dibujos que se acompañan, en los que:

La figura 1 es un diagrama de bloques que muestra las tres entidades principales implicadas cuando se utiliza un procedimiento de acuerdo con la invención.

La figura 2 es un diagrama de bloques que muestra las entidades de la figura 1 para una realización preferida de la invención.

La figura 3a y b son un diagrama de flujo para un procedimiento de acuerdo con una realización preferida de la invención.

La figura 4 es un diagrama de bloques que muestra otra realización de la invención.

La figura 5 es un diagrama de bloques que muestra las unidades para la codificación y decodificación de datos a imagen.

La figura 6 es un dibujo que explica la codificación a imagen del dígito cinco de acuerdo con una posible realización de la invención.

La figura 7 es un esquema de una flecha que representa un mensaje codificado como una imagen con la ayuda de un procedimiento de acuerdo con una realización de la invención.

La figura 8 es un esquema que explica la codificación a imagen del dígito nueve de acuerdo con otra realización de la invención.

Descripción detallada de las realizaciones preferidas

Cuando se trata de la transferencia segura de los comandos de control, se pueden identificar dos modos de fallo. El primer modo de fallo es cuando el comando se pierde o si es erróneo, pero esto es conocido. El segundo modo de fallo es cuando el comando es erróneo, pero esto no es conocido.

Desde un punto de vista general, el segundo modo de fallo es peor que el primero. La solución técnica de las realizaciones de la presente invención se ocupa de los aspectos de seguridad del segundo modo de fallo.

Haciendo referencia a la figura 1, el caso dos anterior se puede generalizar como sigue. Un emisor 110 envía un comando a un receptor 130. Tanto el emisor 110 como el receptor 130 son de alta criticidad, es decir, se consideran, por definición, que pueden manejar los comandos de una manera segura. Los comandos se envían a través de una entidad transferente 120 de baja criticidad, lo que potencialmente puede distorsionar o alterar los datos. Si el comando se ha concebido de tal manera que el receptor 130 puede detectar con una alta probabilidad, que el comando ha sido distorsionado (o falta) y el receptor está provisto de la capacidad de manejar esa situación, el sistema total, es decir, el emisor 110, la entidad transferente 120 y el receptor 130, puede ser considerado como un sistema seguro.

Al juzgar la seguridad de un sistema de acuerdo con lo anterior, es necesario tener en cuenta todos los errores posibles que pueden ser inducidos por la entidad transmisora 120. El sistema debe tener en principio un nivel de seguridad tan alto que incluso si la entidad transferente 120 ha sido concebida para infligir el máximo daño, el sistema deberá poder manejar esto de una manera segura. El siguiente diseño se elaboró para manejar tales casos de una entidad transferente 120 que intenta infligir el máximo daño, y debe poder satisfacer las demandas de las autoridades planteadas por la aeronavegabilidad.

La figura 2 muestra un diagrama de bloques de un sistema de acuerdo con una realización preferida de la invención. Un sistema controlado 230 de alta criticidad envía todos los datos críticos al operador 210 de tal manera que cualquier corrupción de los datos sea detectada por el operador 210. Por ejemplo, se puede usar un procedimiento de comprobación de sumas o un procedimiento en la forma descrita por esta invención. Un procedimiento para que el operador emita un comando al sistema controlado 230 incluye las siguientes etapas:

- El operador 210 envía un comando al sistema controlado 230. Esto puede ser hecho de una forma arbitraria, por ejemplo, como un código de 18 bits.

- El sistema de control envía un mensaje de acuse de recibo del comando al operador 210 a través del enlace de comunicación segura 240 junto con un código de seguridad, que puede ser un número aleatorio. El código de seguridad se envía de una manera tal que se considera que la entidad transferente 220 no ha tenido acceso al código de seguridad. El código puede ser enviado como una imagen o puede estar encriptado.

- El operador 210 comprueba que el sistema de control ha aprehendido el comando correcto, es decir, que la entidad transferente no ha distorsionado los datos.

- Si el operador es de la opinión de que el sistema de control 230 ha capturado el comando correcto, el operador 210 envía en respuesta un mensaje de seguir adelante que comprende el código de seguridad para el sistema de control 230 a través de la entidad transferente 220. Puesto que la entidad transferente 220 no tiene ningún conocimiento del código, se puede argumentar que la entidad transferente no puede generar un código correcto por sí misma.

  En una realización, en la que se envía el código como una imagen, el código en sí es retornado; esto es posible debido a que la entidad transferente no se puede esperar razonablemente a tener en cuenta el código en sí, ya que se envía desde el sistema de control al operador como una imagen. En una realización alternativa, el operador 210, con la ayuda de algunos equipos (no mostrados) descifra un código cifrado y devuelve el código descifrado. Debido a que la entidad transferente 220 no tiene conocimiento de la clave, la entidad transferente 220 no puede tener acceso al código porque fue enviado cifrado desde sistema de control 230 a la entidad transferente 220.

- Cuando el sistema de control 230 ha recibido un código correcto, se ejecuta el comando.

El sistema controlado 230 está concebido de tal manera que sólo acepta un cierto número de códigos enviados por unidad de tiempo. También está concebido para que no acepte los códigos recibidos después de un límite de tiempo máximo después de recibir el comando. Si se reciben demasiados códigos por unidad de tiempo o se reciben códigos demasiado tarde, el sistema 230 realiza una acción predeterminada, como por ejemplo no tener en cuenta el comando y / o alertar al operador 210.

Si el comando del operador se ve distorsionado por la entidad transferente, el operador descubrirá esto cuando el sistema devuelva un acuse de recibo del comando. El operador puede interrumpir la conexión, después de que el sistema controlado 230 tome las medidas adecuadas.

La figura 3 muestra un diagrama de flujo de un procedimiento para la comunicación segura en el sistema de la figura 2. El operador inicia 310 un comando, por ejemplo, tecleándolo. El operador envía 315 un mensaje de comando A al

sistema controlado a través de la entidad transferente. El sistema controlado recibe 320 desde el sistema transferente un mensaje de comando A' que puede ser idéntico al mensaje enviado A o distorsionado o corrompido de alguna manera. Que el mensaje de comando transferido A' está distorsionado o corrompido, o no, no se decide en este punto. El sistema controlado posteriormente crea 325 un código de seguridad SC y un mensaje de reconocimiento ACK. El SC está cifrado formando un código de seguridad cifrado ESC. El ACK se forma concatenando A' y el código de seguridad cifrado ESC. El sistema controlado devuelve 330 el mensaje de acuse de recibo ACK a través de la entidad transferente. Posteriormente, el operador recibe 340 un mensaje de acuse de recibo transferido ACK' que pueden ser idéntico al mensaje de acuse de recibo enviado ACK o distorsionado o corrompido de alguna manera. El operador toma ACK' y separa 345 la porción de mensaje de comando A" y la porción de código de seguridad cifrado transferido ESC'. El operador descifra 350 ESC' y obtiene ESC' descifrado, que a continuación se denomina DESC'.

Comprobando 355 si la porción de mensaje de comando A" es idéntica al mensaje de comando A enviado originalmente, se puede decidir si el mensaje está corrompido o no. Si una porción del mensaje de comando A" es idéntica al mensaje de comando A enviado originalmente, se dice que el mensaje de comando es seguro, es decir, ha sido recibido correctamente por el sistema controlado, y un mensaje de seguir adelante se envía al sistema de control en la forma de CES' DESC' descifrados.

Posteriormente el sistema controlado recibe 365 el DESC' transferido, es decir, DESC", que puede ser idéntico a SC o corrompido de alguna manera. El sistema controlado comprueba 370 si DESC" es idéntico a SC, y si es así, decide que un comando se ha recibido de forma segura y ejecuta 375 el citado comando A.

Si, cuando el operador comprueba 355 si A" es idéntica a A y este no es el caso, el operador decide que no hay una transmisión segura y por lo tanto termina preferiblemente 380 el enlace de datos al sistema controlado. El sistema controlado detecta esta pérdida de enlace de datos y entra en un modo autónomo 382.

Si, cuando el sistema controlado comprueba 370 si DESC" es idéntica a SC, y este no es el caso, el sistema controlado 385 envía un mensaje de error al operador. El sistema controlado no ejecuta 387 el comando correspondiente A. El sistema controlado mantiene continuamente un registro de los números de códigos erróneos que se han recibido durante un período de tiempo que cubre, por ejemplo, los últimos diez segundos. Si este número se hace más grande 390 que un límite predefinido el sistema controlado determina que el enlace de datos no es seguro y entra 392 en un modo autónomo.

La expresión "modo autónomo" significa, para el propósito de la presente solicitud, un modo en el que el sistema controlado, que puede ser un UAV, entra en un modo de auto control y realiza una serie de acciones de seguridad predeterminadas. Las citadas acciones pueden incluir subir a una altura predeterminada, volar a un lugar predeterminado, y aterrizar allí.

Volviendo a la figura 2, en una realización adicional, el sistema controlado está provisto de un transmisor de código periódico, que envía periódicamente un código al operador 210, que, basado en el código, envía una respuesta predeterminada. Esto puede ser implementado como un algoritmo o como un gran conjunto de pares de código - respuesta predeterminados. El operador está provisto de equipo que realiza automáticamente la operación de contestar, pero la cual el operador siempre puede desconectar de forma segura.

Datos codificados de imagen

En una realización preferida adicional, un operador se comunica con un sistema controlado a través de una entidad de transmisión no segura. El sistema controlado está provisto de medios para codificar todos los datos críticos que se van a enviar al operador de una determinada manera que permita al operador descubrir fácilmente los errores de transmisión. En una realización preferida, la información crítica se codifica como una imagen. El formato de imagen se ha concebido de tal forma que si la entidad de transmisión corrompe los datos, el operador lo descubrirá inevitablemente.

La figura 4 es un diagrama de bloques que muestra otra realización de la invención. Un operador 410 utiliza un ordenador personal (PC) 420 comercial disponible en el mercado (COTS) y un equipo de comunicación de enlace inalámbrico para controlar un UAV 430. El operador puede detener la comunicación rompiendo la transmisión de datos al UAV 430 mediante la apertura de una unidad de conmutación 440. La unidad de conmutación 440 puede comprender un interruptor de alimentación al PC y / o equipos de comunicación de enlace inalámbrico 420 o un interruptor de circuito, romper la transmisión sólo en la dirección hacia el UAV 430 o la función de interruptor se puede implementar como sigue:

- Un código aleatorio es generado por el UAV 430
- El código es transmitido al operador 410 a través del enlace inalámbrico y el PC 420

- Como parte del PC 420 se utiliza una unidad que recodifica el código de acuerdo con el conjunto de reglas sólo conocidas por la unidad y el UAV 430.
- Transmite el código recodificado al UAV 430
- En el UAV 430, determina si la recodificación se realiza de acuerdo con las reglas.
- Si la codificación no se hizo de acuerdo con las reglas o si no se recibió ninguna respuesta, el UAV 430 asumirá que los datos ya no se pueden enviar de forma segura.

El operador podrá retirar en cualquier momento la unidad en la descripción anterior para romper la comunicación con el UAV.

Cuando el UAV no recibe mensajes apropiados de seguir adelante, el UAV determina que el enlace de datos no es seguro y entra en un modo autónomo como se ha explicado más arriba. Por lo tanto, de esta manera, el operador siempre tiene, de una manera segura, la capacidad de forzar el UAV al modo autónomo a pesar de la pérdida de la comunicación. Como se ha explicado más arriba, el operador envía comandos al UAV y recibe confirmación en forma de ciertos códigos de seguridad, a partir de los cuales es posible determinar si el comando ha sido recibido correctamente por el UAV, como se ha explicado en detalle más arriba. En una realización preferida, el sistema controlado, por ejemplo un UAV, está provisto de medios para crear un código de seguridad y un mensaje de acuse de recibo como se ha descrito más arriba, en el que el citado código de seguridad está cifrado al codificar el mismo como una o más imagen. Con la expresión "codificar un mensaje como una imagen" significa, con el propósito de la presente solicitud, que una cadena de primer mensaje se transforma en una cadena de segundo mensajes usando un procedimiento de transformación que permite que el mensaje se presente como una imagen, y en el que el citado procedimiento de transformación está concebido de tal manera que cuando la citada imagen se muestra en un órgano de visualización, la imagen permite a un espectador de la citada imagen descubrir errores que han influido en la segunda cadena de mensajes durante, por ejemplo, un proceso de transmisión.

La figura 5 es un diagrama de bloques que muestra las unidades de datos para la codificación y decodificación de imagen. Una unidad emisora 501 está provista de una unidad de datos críticos 505 que maneja los datos críticos. La unidad de datos críticos 505 está conectada a una unidad de codificación de imagen 510 que puede transformar los datos críticos recibidos de la unidad de datos críticos 505, por medio de un procedimiento de transformación que codifica un mensaje de datos críticos como una imagen. La unidad de codificación de imagen 510 está conectada a un transmisor 530 para transmitir el mensaje codificado. La unidad emisora 501 comprende también una unidad de datos no críticos 515 conectada a una unidad de codificación de datos 520 que a su vez está conectada a la unidad transmisora 530.

Una unidad receptora 502 está provista de un receptor 535 para recibir los datos y dividir los datos obtenidos en los datos del código de imagen y en los datos normales de "datos codificados". Los datos de código de imagen se envían a un decodificador de datos de imagen 540 que decodifica los datos y los presenta como una imagen con la ayuda de una unidad de presentación de imagen 545. El receptor 535 también está conectado a un decodificador de datos 550, que está conectado a una unidad de presentación de datos 555, para la presentación de los datos normales no codificados en imagen.

Por ejemplo, si el sistema controlado debe enviar un número entre 0 y 255, este número puede enviarse en un (1) byte. Si la entidad transmisora pudiese corromper estos datos, el operador no podría reconocerlo, debido a que cada corrupción daría lugar a otro número válido. Si, por el contrario, el sistema controlado envía el número como un número de elementos de imagen que tienen que corresponder unos con los otros para crear una imagen continua, el operador puede reconocer que la entidad transmisora ha corrompido los datos, y tomar las medidas adecuadas, por ejemplo, interrumpir la transmisión completamente de tal manera que el sistema controlado descubra esto y tome las medidas apropiadas. La característica de interrumpir la transmisión es crítica y por lo tanto se ha concebído y probado para que sea segura.

Considérese el siguiente ejemplo:

El dígito cinco se va a enviar. La figura 6a y b es un esquema que explica la codificación de imagen del dígito cinco de acuerdo con una posible realización de la invención. El dígito se construye con un número de segmentos. Los segmentos son en forma de líneas rectas cortas que tiene un primer y un segundo extremo. La posición de un extremo de la línea está definida por medio de las coordenadas X e Y. Cada línea se define así por cuatro números, X1, Y1, X2, Y2 correspondientes a las coordenadas X e Y del primer y segundo extremo de la línea, respectivamente.

La Tabla 1 describe un procedimiento para construir el dígito cinco. Una secuencia de transmisión para el dígito cinco sería, por lo tanto: 0,0, 2,0, 2,1, 2,2, 0,3, 2,3, 0,4, 0,5, 0,6, 2,6 .

Tabla 1

Número de línea	X1	Y1	X2	Y2
1	0	0	2	0
2	2	1	2	2
3	0	3	2	3
4	0	4	0	5
5	0	6	2	6

Una transmisión sin fallos daría lugar a la imagen de la figura 6a, y una transmisión introduciendo un fallo puede resultar en la imagen de la figura 6b.

La apariencia de los símbolos transmitidos, por ejemplo, el dígito cinco que se ha descrito, tiene una gran influencia en la capacidad del sistema de proporcionar un procedimiento realmente seguro. Los errores de transmisión individuales no deben dar lugar a otro símbolo válido. Los caracteres de un primer mensaje se pueden elegir entre un conjunto de caracteres alfanuméricos 0 - 9, A - Ö, a - ö. En otra realización, los citados primeros caracteres de mensajes son escogidos de un conjunto de dígitos digitales 0 - 9. En todavía otra realización adicional, los citados primeros caracteres de mensajes son escogidos de un conjunto de dígitos binarios 0 - 1.

En otra realización más se describe un procedimiento para codificar un mensaje de señal crítica que se debe enviar a través de equipos de seguridad no aprobada. La figura 7 muestra una manera para codificar un ángulo, en este caso particular el rumbo de la aeronave, como datos de imagen, es decir, como una flecha que apunta en una rosa de los vientos. La figura 7 muestra una flecha 701 compuesta de seis polígonos 703 - 708.

Los datos de ángulos se convierte en datos de imagen con la ayuda de una tabla o algoritmo en la que los datos de ángulos, por ejemplo, "45" se convierte en seis grupos consecutivos de datos, definiendo cada grupo un polígono de tres o cuatro lados en un sistema de coordenadas X / Y, al definir sus ángulos. A cada polígono también se le puede asignar un color con el fin de mejorar el rendimiento de la interfaz hombre - máquina.

Si la transmisión de alguna manera corrompe la señal de mensaje, esto se hace visualmente detectable en que uno (o más) polígonos recibe una forma que diverge de la forma rectangular y triangular previstas, respectivamente.

La figura 8 muestra el dígito nueve como una imagen definida por un número de píxeles. Cada píxel está definido por una coordenada X y una coordenada Y. El dígito mostrado de este modo se representa por un número, en este caso 15, de pares de coordenadas X / Y. También es posible dar a cada píxel un color mediante la asignación de un código de color como se ha descrito más arriba.

Si en la realización de la figura 8, la transmisión de alguna manera corrompe la señal de mensaje, esto se hará detectable visualmente al operador cuando se visualiza una pantalla que muestra el citado mensaje de señal como una imagen, en la que uno o más píxeles estarán ausentes o en una ubicación diferente de la esperada.

Preferiblemente, la entidad receptora muestra los datos entrantes como elementos gráficos (puntos, píxeles, líneas, polígonos) tal como se recibieron. Las entidades transmisoras están provistas de medios para enviar un mensaje que forma una imagen, a continuación espera un intervalo de tiempo, por ejemplo, 50 ms, a continuación, sobrescribe todos los elementos, dibuja nuevas imágenes, espera 50 ms y así sucesivamente.

En una realización alternativa, la entidad receptora borra automáticamente la imagen después de un cierto tiempo, por ejemplo, después de 50 ms desde que se envió el último elemento.

REIVINDICACIONES

1. Un procedimiento de comunicaciones para permitir la detección de errores de comunicación, comprendiendo el procedimiento las siguientes etapas:

- transformar (510) una cadena del primer mensaje en una cadena del segundo mensaje usando un procedimiento de transformación que permite que el mensaje se presente como una imagen (figura 6a), y en el que el citado procedimiento de transformación está concebida de tal manera que cuando la citada imagen se visualiza en un órgano de visualización, la imagen permite a un observador de la citada imagen descubrir los errores que han influido en la cadena del segunda mensaje;

- transmitir (530) el citado segundo mensaje;

- recibir (535) el citado segundo mensaje;

- exhibir (545) el citado segundo mensaje como una imagen en un órgano de pantalla de visualización;

la citada transformación (510) **se caracteriza por** la etapa de

- convertir los caracteres del primer mensaje a un segundo mensaje utilizando un número de segmentos en forma de líneas rectas que tienen un primer y un segundo extremo, en el que la posición de un extremo de la línea está definida por coordenadas X e Y, y cada línea se define así por cuatro números, X1, Y1, X2, Y2 correspondientes a las coordenadas X e Y de los extremos primero y segundo de la línea, respectivamente.

2. El procedimiento de la reivindicación 1, en el que la citada cadena del primer mensaje es una cadena numérica, y la citada cadena del segundo mensaje es un número de coordenadas X / Y que representan los ángulos de un cierto número de polígonos, y las citadas coordenadas X / Y se eligen de manera que cuando las citadas coordenadas X / Y se utilizan para representar polígonos, los citados polígonos están formando una imagen que representa la información en la citada cadena del primer mensaje.

3. El procedimiento de la reivindicación 1, en el que la citada cadena del primer mensaje comprende caracteres, y la citada cadena del segunda mensaje es un número de grupos de pares de coordenadas X / Y, representando cada grupo un carácter en el citado primer mensaje, y en el que las citadas coordenadas X / Y se eligen de tal manera que cuando se representa una imagen, dejando que cada par de coordenadas X / Y represente un pixel, o el centro de un polígono regular de un cierto tamaño, la citada imagen está formando el citado carácter en el citado primer mensaje.

4. El procedimiento de la reivindicación 1 ó 3, en el que los citados caracteres del primer mensaje son caracteres alfanuméricos 0 - 9, A - Ö, A - ö.

5. El procedimiento de la reivindicación 4, en el que los citados caracteres del primer mensaje son dígitos digitales 0 - 9.

6. El procedimiento de la reivindicación 4, en el que los citados caracteres del primer mensaje son dígitos binarios 0 - 1.

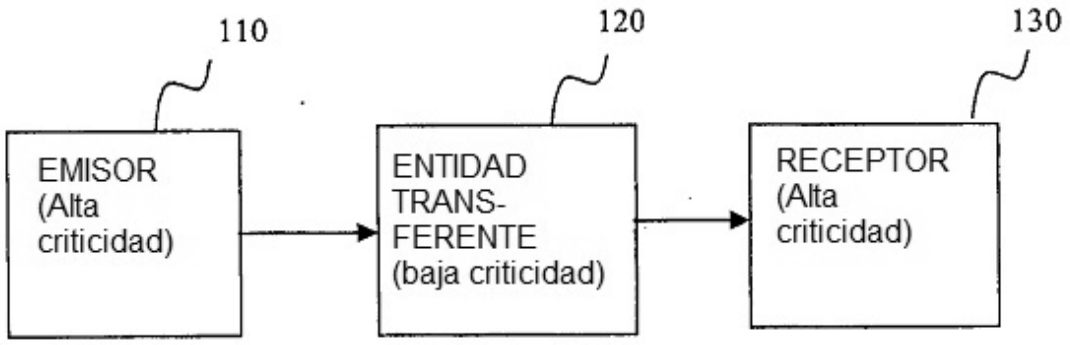
110
120
130
EMISOR
(Alta
criticidad)
ENTIDAD
TRANS-
FERENTE
(baja criticidad)
RECEPTOR
(Alta
criticidad)

Fig. 1

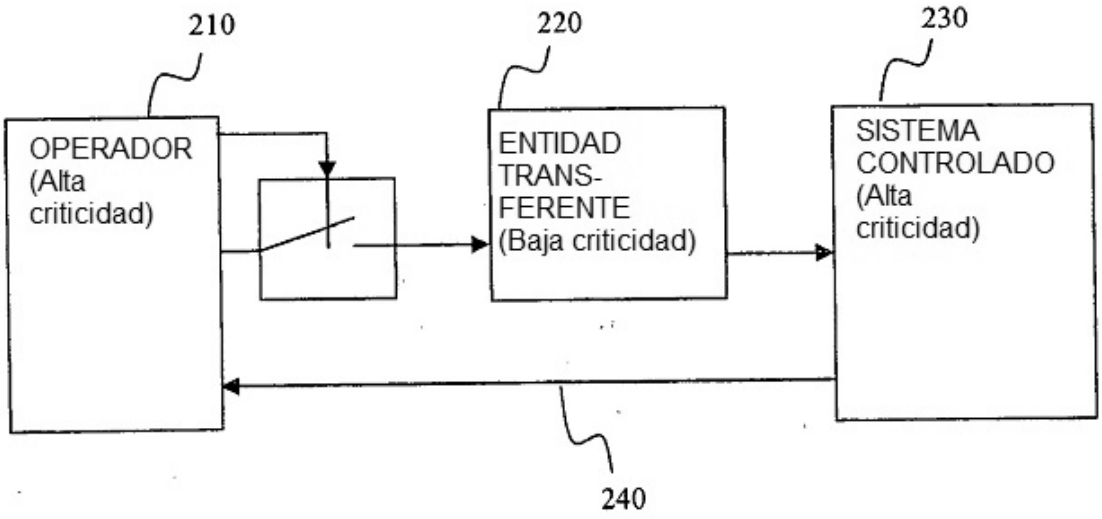
210
220
230
OPERADOR
(Alta
criticidad)
ENTIDAD
TRANS-
FERENTE
(Baja criticidad)
SISTEMA
CONTROLADO
(Alta
criticidad)
240

Fig. 2

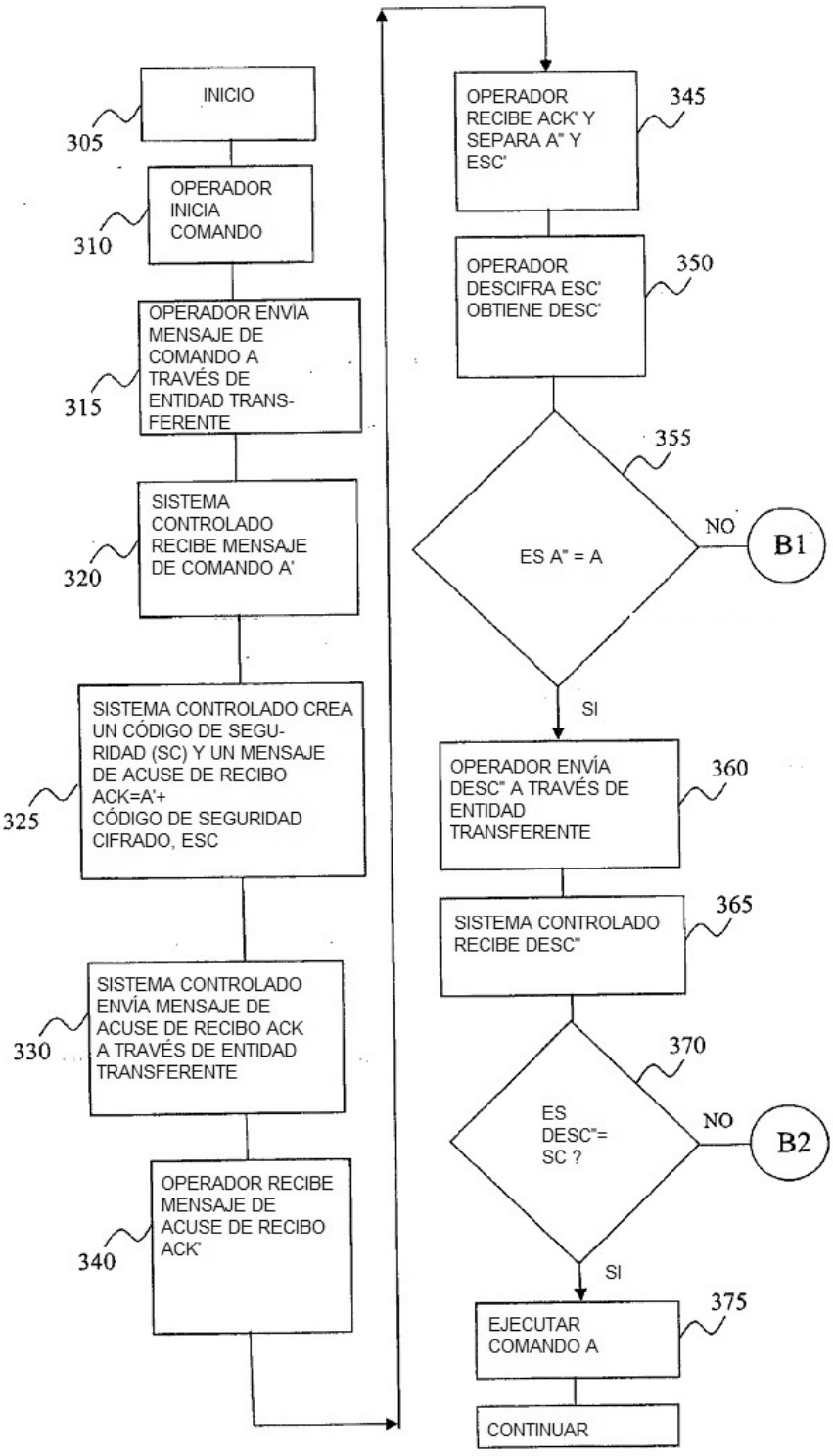
INICIO
305
OPERADOR INICIA COMANDO
310
OPERADOR ENVÍA MENSAJE DE COMANDO A TRAVÉS DE ENTIDAD TRANS-FERENTE
315
SISTEMA CONTROLADO RECIBE MENSAJE DE COMANDO A'
320
SISTEMA CONTROLADO CREA UN CÓDIGO DE SEGU-RIDAD (SC) Y UN MENSAJE DE ACUSE DE RECIBO ACK=A'+ CÓDIGO DE SEGURIDAD CIFRADO, ESC
325
SISTEMA CONTROLADO ENVÍA MENSAJE DE ACUSE DE RECIBO ACK A TRAVÉS DE ENTIDAD TRANSFERENTE
330
OPERADOR RECIBE MENSAJE DE ACUSE DE RECIBO ACK'
340
OPERADOR RECIBE ACK' Y SEPARA A" Y ESC'
345
OPERADOR DESCIFRA ESC' OBTIENE DESC'
350
ES A" = A
355
NO
B1
SI
OPERADOR ENVÍA DESC" A TRAVÉS DE ENTIDAD TRANSFERENTE
360
SISTEMA CONTROLADO RECIBE DESC"
365
ES DESC"= SC ?
370
NO
B2
SI
EJECUTAR COMANDO A
375
CONTINUAR

Fig. 3a

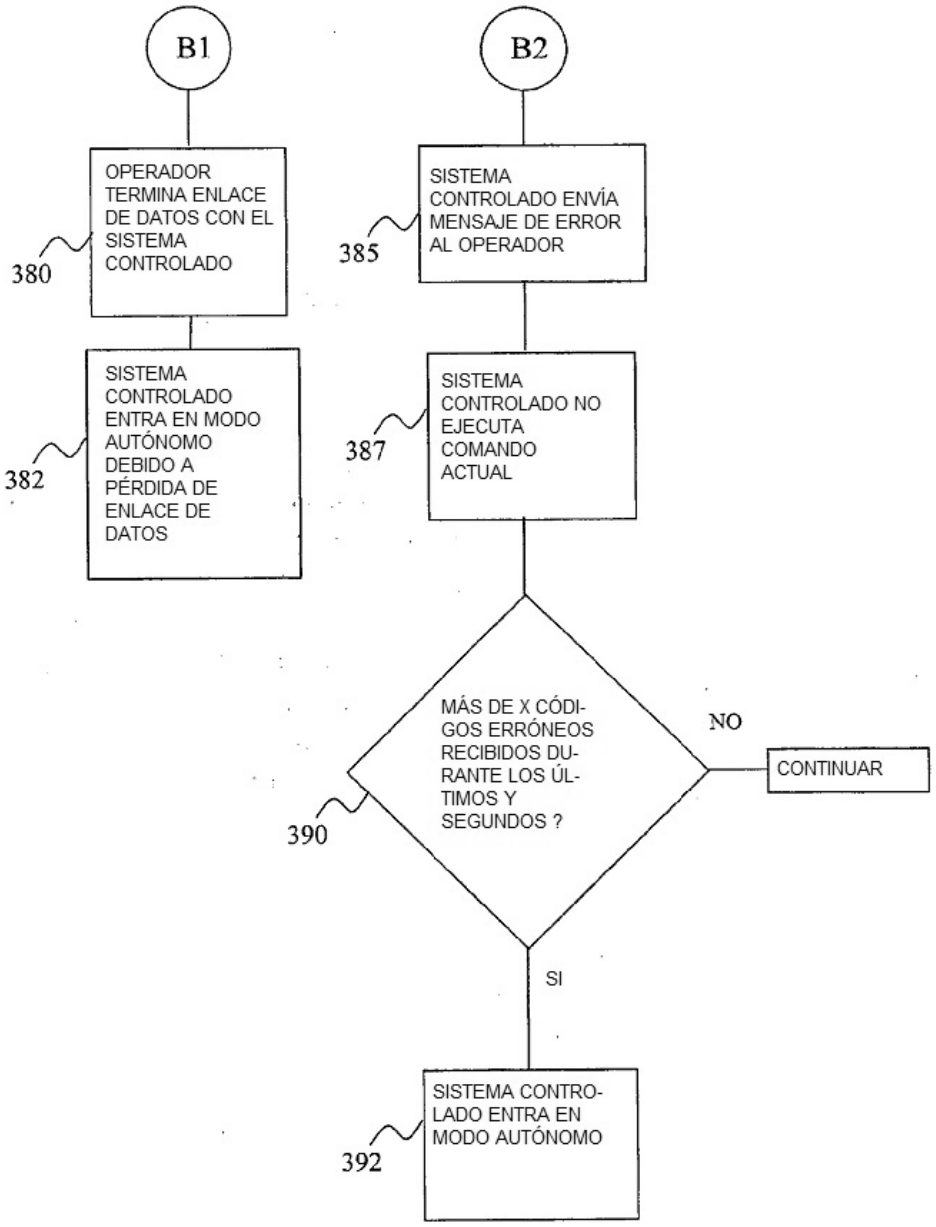
B1
B2
OPERADOR TERMINA ENLACE DE DATOS CON EL SISTEMA CONTROLADO
380
SISTEMA CONTROLADO ENTRA EN MODO AUTÓNOMO DEBIDO A PÉRDIDA DE ENLACE DE DATOS
382
SISTEMA CONTROLADO ENVÍA MENSAJE DE ERROR AL OPERADOR
385
SISTEMA CONTROLADO NO EJECUTA COMANDO ACTUAL
387
MÁS DE X CÓDIGOS ERRÓNEOS RECIBIDOS DURANTE LOS ÚLTIMOS Y SEGUNDOS ?
390
NO
CONTINUAR
SI
SISTEMA CONTROLADO ENTRA EN MODO AUTÓNOMO
392

Fig. 3b

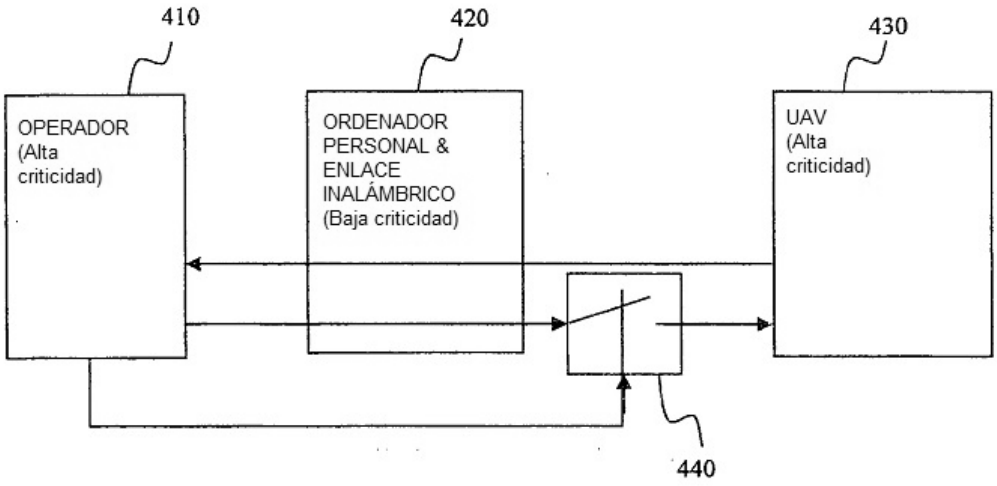

Fig. 4

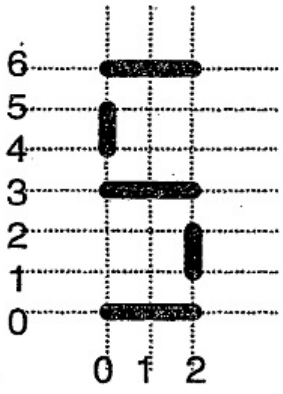

Fig. 6a

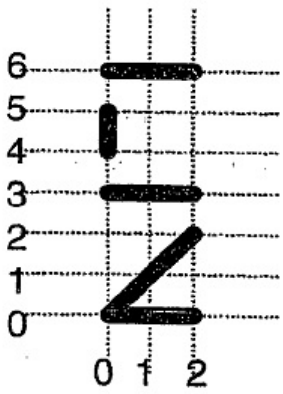

Fig. 6b

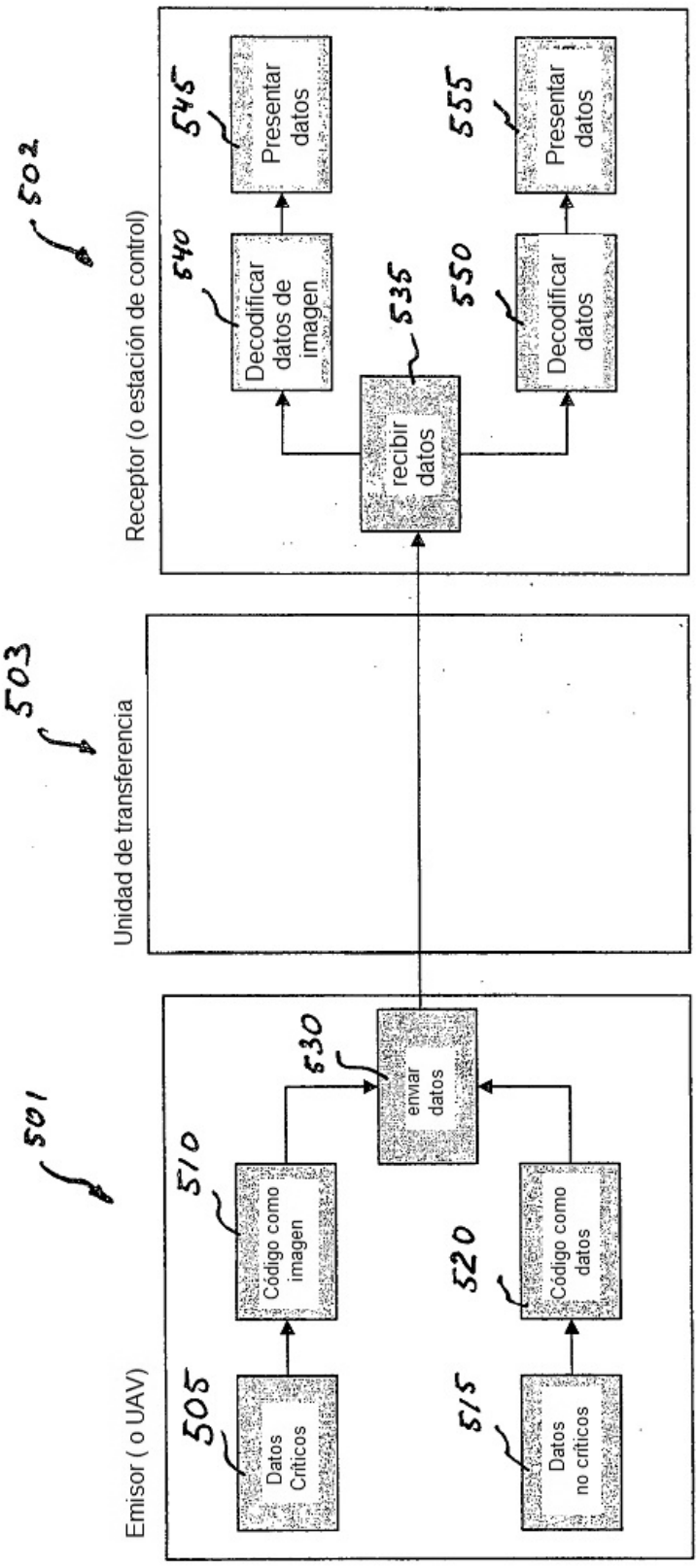
501
Emisor (o UAV)
505
Datos Críticos
510
Código como imagen
515
Datos no críticos
520
Código como datos
530
enviar datos
503
Unidad de transferencia
502
Receptor (o estación de control)
535
recibir datos
540
Decodificar datos de imagen
545
Presentar datos
550
Decodificar datos
555
Presentar datos

Fig. 5

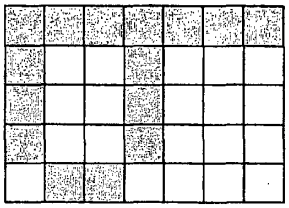

Fig. 8

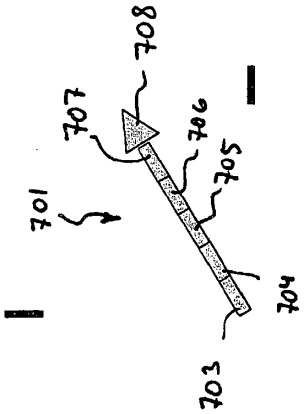

Fig. 7.