(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 372 301**

(51) Int. CI.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06111844 .4**
(96) Fecha de presentación: **28.03.2006**
(97) Número de publicación de la solicitud: **1841163**
(97) Fecha de publicación de la solicitud: **03.10.2007**

(54) Título: **TRANSMISIÓN SEGURA UTILIZANDO EQUIPO DE SEGURIDAD NO APROBADA.**

(45) Fecha de publicación de la mención BOPI:
18.01.2012

(45) Fecha de la publicación del folleto de la patente:
18.01.2012

(73) Titular/es:
SAAB AB
581 88 Linköping, SE

(72) Inventor/es:
Johansson, Rikard;
Eriksson, Jan-Erik y
Stendahl, Peter

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

Transmisión segura utilizando equipo de seguridad no aprobada

Campo de la invención

La presente invención se refiere a procedimientos y dispositivos en sistemas electrónicos para transferir 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 por medio de una entidad de seguridad no aprobada.

Antecedentes

Cuando se desarrolla software de equipos de sistemas de vuelo, es común practicar un estándar conocido como RTCA/DO - 178B. El estándar requiere que los sistemas sean clasificados en lo que respecta al nivel crítico. El estándar requiere que un sistema que puede causar o contribuir a un mal funcionamiento de un cierto grado de seriedad debe ser desarrollado de acuerdo con ciertas reglas. El software se clasifica en cinco niveles, de A a E, en los que el nivel A se corresponde al más crítico, y E es el nivel menos crítico. El costo del desarrollo de software de clase A y B, es aproximadamente tres veces el costo del desarrollo de software de clase D. No hay requisitos en el RTCA/DO - 178B para el software de clase E, por lo que es difícil comparar los costos. El software debe ser desarrollado de acuerdo con la clase A, si un error de software puede producir un choque con víctimas, de acuerdo con la clase B si el error puede producir graves lesiones personales o a niveles de seguridad gravemente reducidos y otros niveles adicionales C, D, E que corresponden a efectos menos severos de un error.

En muchas aplicaciones, la información errónea puede conducir a consecuencias muy graves (en estas aplicaciones, se debería aplicar el software de clase A). Como ejemplo, considérese un caso en el que se envió información errónea a un sistema de armas, lo que condujo a disparar erróneamente.

El software clasificado como tipo A o B es caro de desarrollar y, en principio, no se permite que se integren o se ejecuten en un ordenador comercial que utiliza software comercialmente disponible (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 en clase A o B, para el tipo de funciones que se han mencionado con anterioridad.

En relación con la introducción de Vehículos Aéreos No Tripulados (UAV), hay una necesidad de controlar con seguridad estos vehículos utilizando principalmente los productos COTS. Esto no es una alternativa si se va a utilizar el procedimiento tradicional, en comparación con el anterior, para conseguir un flujo seguro de información. También en otras aplicaciones, el procedimiento tradicional origina un mayor costo económico que lo que sería el caso si los productos tuviesen una clase de criticidad inferior a A o B, o lo que sería el caso si se pudiesen utilizar los productos COTS, tanto en hardware como en software.

Una aplicación típica de la invención es hacer posible controlar remotamente un UAV utilizando (en parte) productos de software y ordenadores de bajo costo COTS cumpliendo al mismo tiempo los requisitos de los estándares de seguridad aplicables, tales como RTCA/DO - 178B.

El documento US 2003/130770 A1 desvela un procedimiento para asumir y mantener el control remoto seguro de una aeronave en caso de un ataque, o de la incapacidad del piloto de la aeronave. El procedimiento incluye los etapas de: proporcionar un enlace de transmisión segura entre una localización remota y la aeronave; transmitir un comando a la aeronave para interrumpir el control del piloto; transmitir datos de vuelo de la aeronave a la localización remota; transmitir datos de control a la aeronave; mantener el control remoto hasta que la necesidad de control remoto haya terminado.

Un objeto de la presente invención es proporcionar un procedimiento para la comunicación en sistemas críticos de seguridad sin tener que usar equipos de seguridad aprobados en toda la cadena de comunicación, mientras todavía pudiendo cumplir con los estándares de seguridad aplicables, tales como el RTCA/DO - 178B .

Sumario de la invención

El objeto anterior se alcanza por medio de un procedimiento de comunicación de acuerdo con la reivindicación 1. El procedimiento comprende las siguientes etapas:

- enviar un mensaje de comando desde una primera entidad a una segunda entidad por medio de una tercera entidad;
- devolver desde la segunda entidad a la primera entidad, un mensaje de acuse de recibo del primer mensaje que comprende un código de seguridad encriptado;
- comprobar, por la primera entidad, que el mensaje de acuse de recibo devuelto corresponde al mensaje enviado originalmente; descifrando el citado mensaje de acuse de recibo y comprobando que son idénticos;

- si es así, devolver un mensaje de autorización para proceder, que comprende el código de seguridad encriptado recibido descifrado desde la primera entidad a la segunda entidad por medio de la tercera entidad;

- en la segunda entidad, decidir si el código de seguridad recibido es correcto.

- si el código de seguridad es correcto, el comando de acuerdo con el mensaje enviado originalmente desde la primera entidad, es ejecutado.

En una realización adicional, el procedimiento comprende, además, las siguientes etapas para la detección de la pérdida de las comunicaciones:

- enviar continuamente desde la segunda entidad, códigos únicos.

- calcular y enviar continuamente en la primera entidad, los valores de retorno para cada código único basado en un algoritmo determinado.

- verificar continuamente en la segunda entidad, que el valor de retorno calculado desde la primera entidad es correcto. Si no es así, la segunda entidad debe llevar a cabo acciones predeterminadas, debido a la pérdida de comunicación con la primera entidad.

- si durante la transmisión de mensajes desde la primera entidad a la segunda entidad, la primera entidad encuentra que el mensaje de acuse de recibo retornado no se corresponde con el mensaje enviado, la primera entidad interrumpirá el cálculo del valor de retorno, lo que obliga a la segunda entidad a tomar acciones predeterminadas, debido a la pérdida de comunicación.

En otra realización preferida, el mensaje es un comando seleccionado de un conjunto limitado de comandos.

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 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 en una realización preferida de la invención.

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

Descripción detallada de 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 si el comando se pierde o si es errónea, pero esto es conocido. El segundo modo de fallo es cuando el comando es erróneo, pero esto NO es conocido.

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

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

Cuando se juzga 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, en principio, debe tener un alto nivel de seguridad que, incluso si la entidad de transferencia 120 ha sido diseñada para infligir el daño máximo, el sistema deberá poder manejar esto de una manera segura. El siguiente diseño está concebido para tratar tales casos de una entidad de transferencia 120 de infligir daño máximo, y debe poder cumplir las demandas planteadas por las autoridades de 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 criticidad alta envía todos los datos críticos al operador 210, de tal manera que cualquier corrupción de los datos será detectada por el operador 210. Por ejemplo, se puede utilizar un procedimiento de

comprobación o la información puede ser enviada como una imagen. 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 se puede realizar de una manera arbitraria, por ejemplo, como un código de 18 bits.

- El sistema controlado envía un mensaje de acuse de recibo del comando al operador 210 por medio del enlace de comunicación de seguridad 240, junto con un código de seguridad, que puede ser un número aleatorio. El código de seguridad se envía de tal manera que se considera que la entidad de transferencia 220 no tiene acceso al código de seguridad. El código puede ser enviado como una imagen o puede ser encriptado.

- El operador 210 comprueba que el sistema controlado ha capturado el comando correcto, es decir, que la entidad de transferencia no ha distorsionado los datos.

- Si el operador es de la opinión que el sistema controlado 230 ha capturado el comando correcto, el operador 210 envía como respuesta un mensaje de autorización para proceder que comprende el código de seguridad, al sistema controlado 230 por medio de la entidad de transmisión 220. Puesto que la entidad de transferencia 220 no tiene ningún conocimiento del código, se puede argumentar que la entidad de transferencia no puede generar un código correcto por sí misma.

En una realización en la que el código enviado era una imagen, el propio código se devuelve; esto es posible porque no se puede esperar razonablemente que la entidad de transferencia sea conscientes del propio código, ya que fue enviado desde el sistema controlado 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 de transferencia 220 no tiene conocimiento de la clave, la entidad de transferencia 220 no puede acceder al código, ya que se envió cifrado desde el sistema controlado 230 a la entidad de transferencia 220.

- Cuando el sistema controlado 230 ha recibido un código correcto, ejecuta el comando.

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

Si el comando del operador es distorsionado por la entidad de transferencia, el operador descubrirá esto cuando el sistema devuelva un acuse de recibo del comando. El operador puede interrumpir entonces la conexión, con lo que posteriormente el sistema controlado 230 tomará las acciones 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, escribiéndolo El operador envía 315 un mensaje de comando A al sistema controlado por medio de la entidad de transferencia. El sistema controlado recibe 320 del sistema de transferencia, un mensaje de comando A’ que puede ser idéntico al mensaje enviado A o estar distorsionado o corrompido de alguna manera. Si el mensaje de comando transferido A' está distorsionado o corrompido, o no, no se decide en este momento. El sistema controlado posteriormente crea 325 un código de seguridad SC y un mensaje de acuse de recibo ACK. SC se codifica formando un código de seguridad cifrado ESC. ACK se forma por la concatenación de A' y el código de seguridad cifrado ESC. El sistema de control devuelve 330 el mensaje de acuse de recibo ACK por medio de la entidad de transferencia. Posteriormente, el operador recibe 340 el mensaje de acuse de recibo transferido ACK', que puede ser idéntico al mensaje de acuse de recibo enviado ACK o estar distorsionada o corrompido de alguna manera. El operador toma ACK' y separa 345 la porción A" del mensaje de comando y la porción ESC' del código de seguridad cifrado transferido. El operador descodifica 350 ESC' y obtiene ESC' descifrado, aquí denominado DESC’.

Al comprobar 355 si la porción de mensaje de comando A" es idéntico al mensaje de comando A enviado originalmente, se puede decidir si el mensaje está corrompido o no. Si la porción de 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 autorización para proceder es enviado al sistema controlado en la forma del ESC' descifrado, DESC'.

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

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

Si cuando el sistema controlado comprueba 370 si DESC" es idéntico a SC y este no es el caso, el sistema controlado envía 385 un mensaje de error al operador. El sistema controlado no ejecuta 387 el comando correspondiente A. El sistema controlado mantiene un seguimiento continuo del número de códigos erróneos que se han recibido durante un periodo de tiempo que cubre, por ejemplo, los últimos diez segundos. Si este número aumenta de tamaño 390 con respecto a un límite predefinido el sistema controlado determina que el enlace de datos no es seguro y entra 392 en un modo autónomo.

Un "modo autónomo", con el propósito de la presente solicitud, significa un modo en el que el sistema controlado, que puede ser un UAV, entra en un modo autocontrolado y realiza una serie de acciones de seguridad predeterminadas. Las citadas acciones pueden incluir subir a una altura predeterminada, volar a una localización predeterminada, 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, en base al código, envía una respuesta predeterminada. Esto puede ser implementado como un algoritmo o como un conjunto grande de pares de respuestas cifradas predeterminadas. El operador está provisto de equipo que realiza automáticamente la operación de respuesta, pero el operador siempre puede desconectarlo de una manera segura.

REIVINDICACIONES

1. Un procedimiento de comunicación para uso en un equipo de sistema RTCA/DO - 178B de tipo A o B, para comunicar con seguridad un mensaje desde una primera entidad de seguridad aprobada (210) a una segunda entidad de seguridad aprobada (230) por medio de una tercera entidad de seguridad no aprobada, que comprende las siguientes etapas:

   - enviar (315) un mensaje de comando desde la primera entidad (210) a la segunda entidad (230) por medio de la tercera entidad (220);

   - devolver (330, 325), desde la segunda entidad (230) a la primera entidad (210) un mensaje de acuse de recibo del primer mensaje que comprende un código de seguridad cifrado;

   - comprobar (355), en la primera entidad, que el mensaje de acuse de recibo devuelto corresponde al mensaje enviado originalmente, al descifrar (350) el citado código de seguridad encriptado del citado mensaje de acuse de recibo y comprobar que una porción del mensaje de comando del citado mensaje de acuse de recibo con el citado mensaje de comando enviado son idénticos;

   - si es así, devolver (360), desde la primera entidad a la segunda entidad un mensaje de autorización para proceder, que comprende el código de seguridad encriptado recibido descifrado;

   - decidir (370), en la segunda entidad (230), si el código de seguridad recibido corresponde al enviado a la primera entidad, y si es así, determinar que es seguro ejecutar el citado mensaje de comando;

   - si es así, ejecutar (375) el comando actual;

   - si no es así, no ejecutar (387) el comando actual.

2. El procedimiento de comunicaciones de la reivindicación 1, que comprende, además, un procedimiento para detectar la pérdida de comunicaciones.

3. El procedimiento de comunicaciones de la reivindicación 2, en el que el citado procedimiento comprende las siguientes etapas:

   - desde la segunda entidad, enviar continuamente un código único;

   - en la primera entidad, calcular continuamente un valor de retorno basado en algún algoritmo;

   - en la segunda entidad, verificar continuamente que el valor de retorno calculado desde la primera entidad es correcto, si no es así, la segunda entidad deberá adoptar medidas adecuadas debido a la pérdida de comunicación con primera entidad;

   - si durante la transmisión de mensajes desde la primera entidad a la segunda entidad, la primera entidad encuentra que el mensaje de acuse de recibo retornado no se corresponde con el mensaje enviado, la primera entidad interrumpirá el cálculo del citado valor de retorno, lo que obligará a la segunda entidad a adoptar la acción adecuada debido a la pérdida de comunicación.

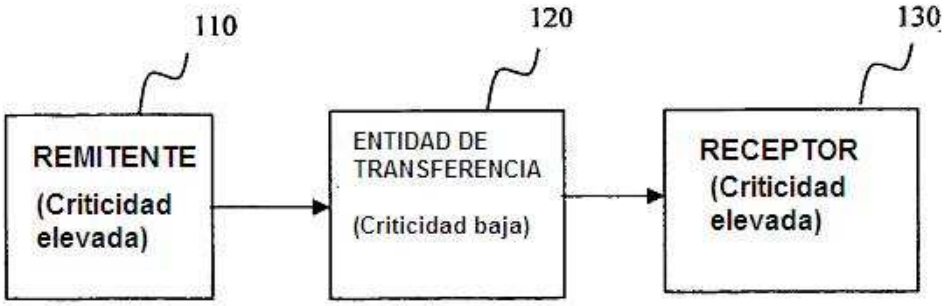
110
120
130
REMITENTE
(Criticidad elevada)
ENTIDAD DE TRANSFERENCIA
(Criticidad baja)
RECEPTOR
(Criticidad elevada)

Fig. 1

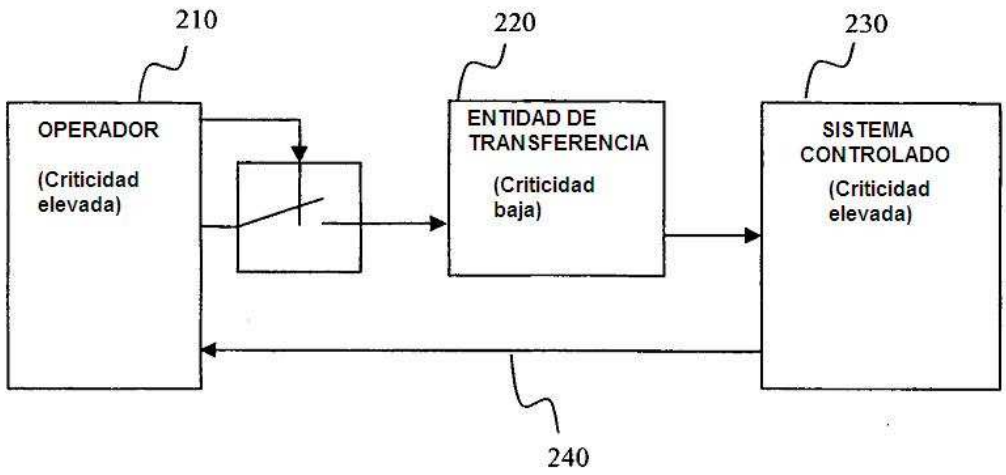
210
220
230
OPERADOR
(Criticidad elevada)
ENTIDAD DE TRANSFERENCIA
(Criticidad baja)
SISTEMA CONTROLADO
(Criticidad elevada)
240

Fig. 2

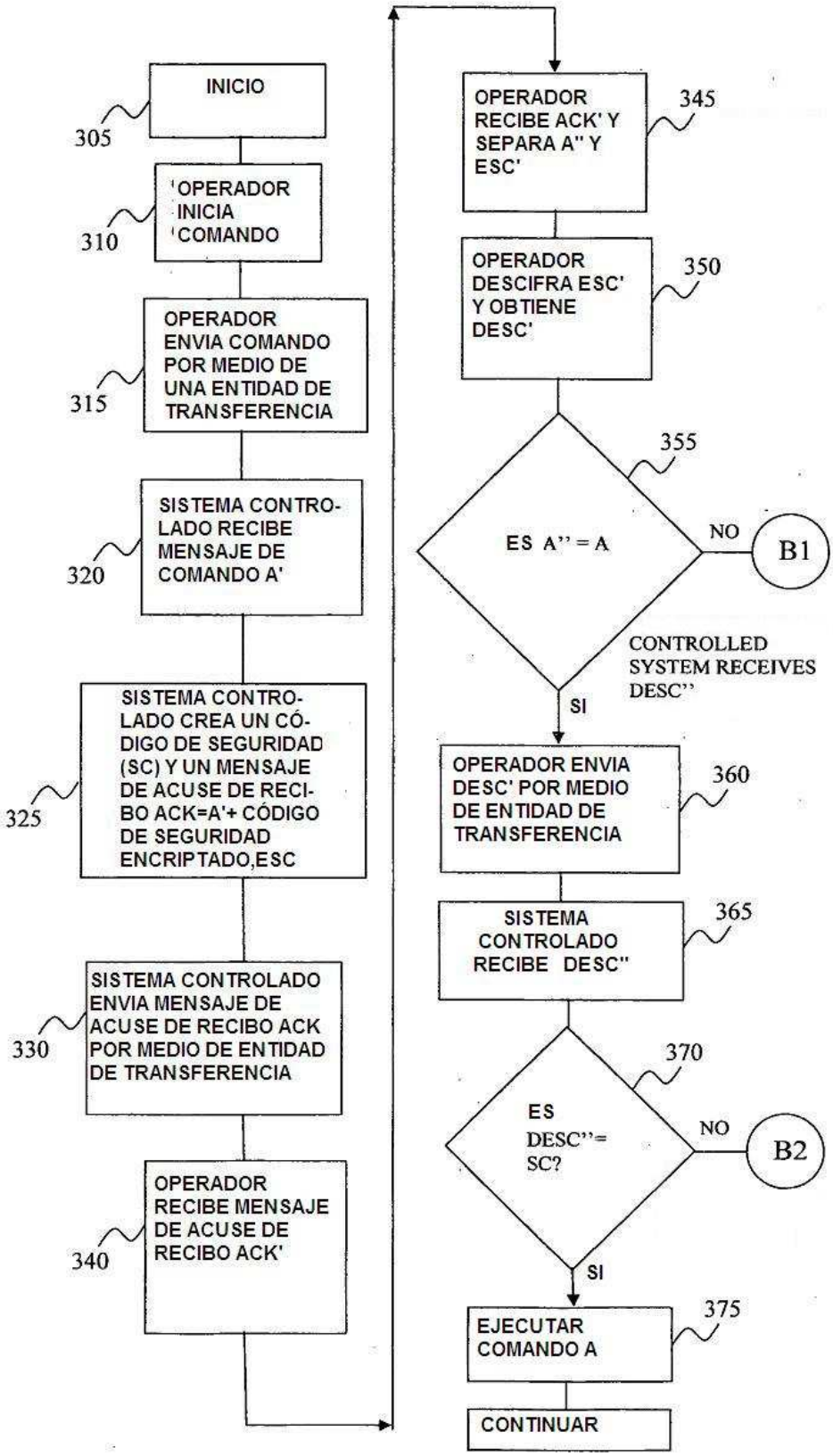
INICIO
305
OPERADOR INICIA COMANDO
310
OPERADOR ENVIA COMANDO POR MEDIO DE UNA ENTIDAD DE TRANSFERENCIA
315
SISTEMA CONTRO-LADO RECIBE MENSAJE DE COMANDO A'
320
SISTEMA CONTRO-LADO CREA UN CÓ-DIGO DE SEGURIDAD (SC) Y UN MENSAJE DE ACUSE DE RECI-BO ACK=A'+ CÓDIGO DE SEGURIDAD ENCRIPTADO,ESC
325
SISTEMA CONTROLADO ENVIA MENSAJE DE ACUSE DE RECIBO ACK POR MEDIO DE ENTIDAD DE TRANSFERENCIA
330
OPERADOR RECIBE MENSAJE DE ACUSE DE RECIBO ACK'
340
OPERADOR RECIBE ACK' Y SEPARA A'' Y ESC'
345
OPERADOR DESCIFRA ESC' Y OBTIENE DESC'
350
ES A'' = A
355
NO
B1
CONTROLLED SYSTEM RECEIVES DESC''
SI
OPERADOR ENVIA DESC' POR MEDIO DE ENTIDAD DE TRANSFERENCIA
360
SISTEMA CONTROLADO RECIBE DESC''
365
ES DESC''= SC?
370
NO
B2
SI
EJECUTAR COMANDO A
375
CONTINUAR

Fig. 3a

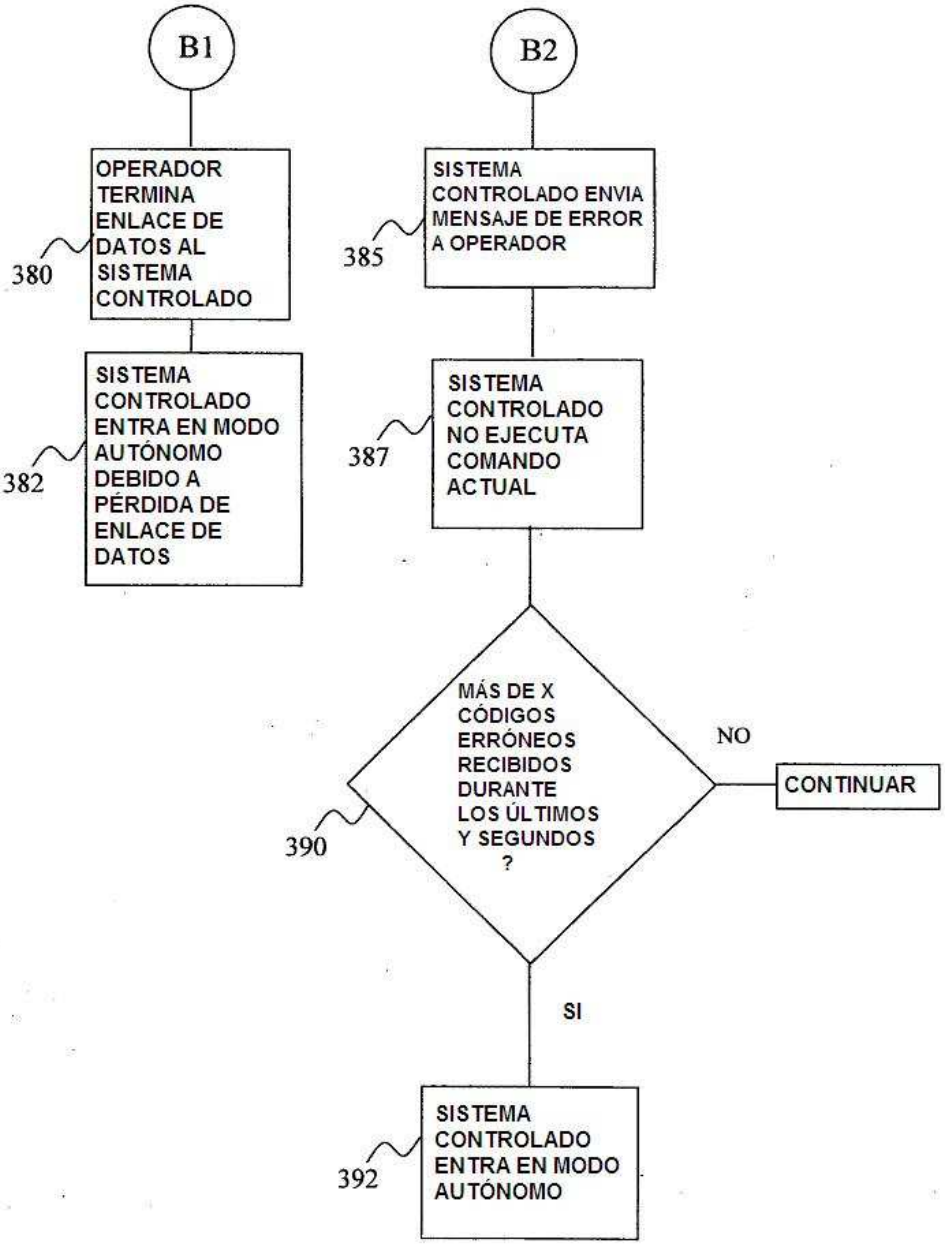
B1
B2
OPERADOR TERMINA ENLACE DE DATOS AL SISTEMA CONTROLADO
380
SISTEMA CONTROLADO ENTRA EN MODO AUTÓNOMO DEBIDO A PÉRDIDA DE ENLACE DE DATOS
382
SISTEMA CONTROLADO ENVIA MENSAJE DE ERROR A OPERADOR
385
SISTEMA CONTROLADO NO EJECUTA COMANDO ACTUAL
387
MÁS DE X CÓDIGOS ERRÓNEOS RECIBIDOS DURANTE LOS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

Fig. 3b