(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 742 128**

(51) Int. CI.:

H04L 29/06 (2006.01)
B64F 5/60 (2007.01)
B64C 39/02 (2006.01)
G06F 21/44 (2013.01)
H04W 12/06 (2009.01)
H04W 4/70 (2008.01)
H04W 4/80 (2008.01)
B64D 45/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.03.2017 E 17382110 (9)**

(97) Fecha y número de publicación de la concesión europea: **15.05.2019 EP 3370386**

(54) Título: **Sistema y método implementado por ordenador para la autentificación entre máquinas de un aparato**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.02.2020

(73) Titular/es:

THE BOEING COMPANY (100.0%)
100 North Riverside Plaza
Chicago, IL 60606-2016, US

(72) Inventor/es:

PEREZ VILLAR, VICTOR y
KAWIECKI, GRZEGORZ M.

DESCRIPCIÓN

Sistema y método implementado por ordenador para la autentificación entre máquinas de un aparato

Campo

La presente divulgación está comprendida en el campo de la seguridad en las telecomunicaciones. Más particularmente, se refiere a autentificación entre máquinas (M2M) que usa un mecanismo de autentificación de múltiples factores (MFA) mejorado.

Antecedentes

La autentificación es el procedimiento de determinación de si alguien o algo es, de hecho, quien o lo que afirma ser. De manera tradicional, la autentificación se ha centrado en interacciones entre ser humano y máquina, de modo que la máquina verifica automáticamente la validez de un usuario identificado. Recientemente, la autentificación también está destinada a entornos entre máquinas (por ejemplo, servicios de soporte en línea, sensores de telemedicina, y redes inteligentes). Para este fin, se adoptan varias técnicas.

Las tecnologías de autentificación basada en certificación garantizan la autentificación usando una clave de encriptación pública y privada que es única. Estos testigos también pueden usarse para firmar transacciones digitalmente. Normalmente, una autoridad de certificación (CA) es responsable de emitir y verificar certificados digitales como parte de la infraestructura de clave pública.

También existen tecnologías basadas en autentificación basada en contexto que usa información contextual, por ejemplo, posición de GPS, para determinar si una identidad de sistema es auténtica o no. Sin embargo, la autentificación basada en contexto por sí sola no es suficiente y, habitualmente, es complementaria a otras fuertes técnicas de autentificación.

Existen otras herramientas de autentificación, como testigos de hardware y software que generan números aleatorios o cadenas de caracteres que cambian a intervalos muy cortos de tiempo y se sincronizan con el sistema de autentificación. Sin embargo, este tipo de herramientas de autentificación necesitan conectarse a un sistema de autentificación, lo que resulta un fuerte requisito que no puede cumplirse fácilmente.

Del mismo modo, existen herramientas de autentificación que no son adecuadas para un entorno entre máquinas porque están destinadas a seres humanos (por ejemplo, impugnación/respuesta, autentificación biométrica, o comunicación fuera de banda).

Los certificados digitales no son suficientes para la autentificación en muchas circunstancias. Por ejemplo, no son útiles para sistemas aéreos no tripulados (UAS) dado que la plataforma puede portar muchas cargas útiles operacionales, y los certificados digitales no garantizan un uso seguro de cargas útiles añadidas.

Las tecnologías de autentificación de múltiples factores (MFA) se basan en contraseñas de un solo uso que usan un secreto compartido o semilla que se almacena en el dispositivo de autentificación integrado y en la base de datos de autentificación. Esta técnica garantiza la autentificación generando una contraseña de un solo uso basándose en el secreto del testigo.

En resumen, muchas de las tecnologías disponibles actualmente para identificar la verificación no son completamente funcionales en entornos M2M. De manera tradicional, necesitan dirigirse tres preguntas: “qué sabes, qué tienes, y quién eres”. Dado que las tecnologías actuales se basan en una participación humana y asumen que la entidad que se autentifica es una persona, o que un ser humano está relacionado con los procedimientos de autentificación, experimentan diversas limitaciones. En particular, el no poder proporcionar una respuesta apropiada a la pregunta “quién eres” o, en este caso, “qué es el aparato”.

El documento WO2016/025044 de la técnica anterior da a conocer una utilidad de configuración que se usa para configurar módulos de carga útil y de vuelo de un UAV. Las configuraciones pueden cargarse a partir de y guardarse en archivos de configuración. Una configuración puede validarse frente a una configuración de UAV real. Sin embargo, no se da a conocer la medición y análisis de características de comportamiento o físicas únicas con el fin de verificar la identidad de los módulos.

Sumario

Una revisión de la técnica anterior muestra que existe una necesidad de un sistema y un método para la autentificación entre máquinas (M2M) de múltiples factores (MFA). La invención se expone en las reivindicaciones adjuntas. La invención se define mediante las reivindicaciones adjuntas. Las reivindicaciones dependientes definen realizaciones ventajosas. Las realizaciones y/o ejemplos de la siguiente descripción, que no están cubiertas por las reivindicaciones adjuntas, se considera que no forman parte de la presente invención.

Un conmutador para llamadas hipotéticas M2M para modificaciones profundas en técnicas de autentificación existentes. Algunas de las enseñanzas de esta divulgación ofrecen un nuevo modelo ampliando de manera

estratégica el concepto biométrico, es decir, la medición y análisis de características de comportamiento o físicas únicas para verificar fines de identificación, para interacciones entre máquinas. Este nuevo concepto puede denominarse “maquinométrico”.

En general, la presente divulgación tiene el objetivo de permitir que ordenadores y otros dispositivos interaccionen entre sí e intercambien información autorizada de manera automática sin intervención humana y de manera segura.

Dejando de lado ese objetivo, un objeto de la presente divulgación se refiere a técnicas que gestionan adiciones de terceros (subsistemas de terceros) en un aparato y tiene el objetivo de reducir la probabilidad de autentificación de un aparato con una componente comprometida.

Incluso otro objeto es proporcionar un mecanismo para una mejor detección de cualquier violación de la seguridad del sistema en sistemas fiables, o componente comprometidas.

Otro objeto de la presente divulgación se refiere a técnicas que garantizan la integridad de operaciones sin afectar negativamente en la autonomía. La autonomía debe comprenderse en esta divulgación como la capacidad para funcionar de manera independiente del control humano.

Las técnicas dadas a conocer mejoran significativamente la seguridad y eliminan la necesidad de intervención humana, lo que resulta apropiado para la mayor parte de los sistemas que no están destinados a seres humanos. En particular, los UAS pueden beneficiarse de conceptos dados a conocer en este documento para garantizar la integridad de misiones. Los sistemas marinos no tripulados, la recogida de objetos y el intercambio de datos dentro del entorno integrado de Internet de las cosas, autómatas industriales con elementos de autonomía, agentes de software autónomos, tales como determinadas herramientas de intercambio de inventario y otros sistemas que demandan un alto nivel de autonomía también pueden beneficiarse de esta divulgación.

Objetos y ventajas adicionales de la presente invención resultarán evidentes a partir de la siguiente descripción detallada, haciéndose referencia a los dibujos adjuntos en los que se ilustran de manera clara las realizaciones preferidas.

Breve descripción de los dibujos

Una serie de dibujos que ayudan a una mejor comprensión de la divulgación y que se presentan como ejemplos no limitativos y se describen muy brevemente a continuación.

La figura 1 muestra esquemáticamente un diagrama a modo de ejemplo de un sistema según una realización.

La figura 2A muestra esquemáticamente un aparato con diversos componentes críticos.

La figura 2B muestra esquemáticamente el aparato de la figura 2A con un componente malicioso.

La figura 3A muestra esquemáticamente una red de dependencia para componentes seleccionados de un UAS.

La figura 3B es un diagrama que muestra dependencias próximas de dos componentes en la figura 3A.

La figura 4 muestra una posible clasificación de diferentes tipos de firmas.

La figura 5 muestra esquemáticamente una región de autentificación positiva en un espacio de firma tridimensional.

La figura 6 describe esquemáticamente un procedimiento para la autentificación autónoma de un aparato.

La figura 7 describe esquemáticamente un subprocedimiento de la figura 6 para la autentificación de múltiples factores de una componente de un aparato.

La figura 8 describe esquemáticamente una arquitectura de transmisión de datos para implementar la autentificación de componente.

La figura 9 describe esquemáticamente una arquitectura a modo de ejemplo para implementar la autentificación de componente para componentes de UAV seleccionados.

Descripción detallada

Con fines de explicación, se exponen detalles específicos con el fin de proporcionar una comprensión meticulosa de la presente divulgación. Sin embargo, es evidente para un experto en la técnica que la presente divulgación puede llevarse a la práctica sin estos detalles específicos o con disposiciones equivalentes.

Particularmente, las técnicas de autentificación propuestas pueden aplicarse a todas las categorías de vehículos tripulados y no tripulados, conjuntos de vehículos no tripulados, autómatas industriales con elementos de autonomía, agentes de software autónomos, tales como herramientas de gestión de acciones seleccionadas y el Internet de las cosas, en general. Sin embargo, se explicará, en su mayoría, usando sistemas aéreos no tripulados (UAS) dado que

sirven para explicar una variedad de operaciones en situaciones complejas con actualizaciones que deben realizarse de manera frecuente.

La figura 1 es un diagrama de bloques de un sistema 100 que puede proporcionar autentificación M2M de múltiples factores a un componente 102 crítico de un aparato 110 y, por tanto, al propio aparato. En la figura 1 se muestran estructuras y dispositivos que se conocen bien en forma de bloques para evitar complicar de manera innecesaria la presente divulgación. Una base 140 de datos de configuración almacena una selección de componentes críticos. La base 140 de datos se ilustra de manera independiente, sin embargo, puede formar parte del sistema 100. Alternativamente, la base 140 de datos puede formar parte del propio aparato 110. De manera similar, el sistema 100 puede tener determinadas unidades instaladas en el aparato 110.

Puede ser deseable que, antes de la ejecución de una función o tarea por el aparato 110, se cumplan determinadas condiciones. Estas condiciones se refieren, principalmente, a la autentificación de componentes críticos, tales como el componente 102 del aparato 110 relacionado con la realización de tal función. La autentificación proporcionada por el sistema 100 sirve para este fin.

El aparato 110 se autentifica cuando se autentifican de manera válida determinado número de componentes 102 críticos. De esta forma, la autentificación puede establecerse en dos niveles diferente. En el nivel superior, con el fin de autenticar cada componente 102 crítico, se tienen en consideración uno o más componentes 104 secundarios que tienen relación con un componente 102 crítico. Una red de dependencia puede definirse, por tanto, según la relación entre diferentes componentes 102, 104. En un nivel inferior, cada componente puede requerir una autentificación de factor k. Es decir, k diferentes firmas del componente deben comprobarse de manera válida.

Haciendo referencia de nuevo a la figura 1, el aparato 110 se controla para realizar una función que implica al primer componente 102. Para permitir esta función, se requiere una autentificación M2M. Inicialmente, una unidad 120 de recuperación del sistema 100 envía una solicitud de autentificación al aparato 110 con respecto al primer componente 102. Adicionalmente, la unidad 120 de recuperación también recupera una lista de dependencias almacenada en una base 140 de datos de configuración. La lista de dependencias comprende información de autentificación del primer componente 102 y uno o más componentes 104 adicionales asociados con el primer componente 102. La información de autentificación en la lista de dependencias incluye valores almacenados para firmas físicas y firmas digitales de los componentes 104, 102.

Una unidad 160 de adquisición en el sistema 100 adquiere firmas presentes para el primer componente 102 y para cada componente 104 dependiente presente en la lista de dependencias. Las firmas físicas pueden adquirirse por medio de sensores. En particular, si el aparato 110 incluye un sistema de gestión de salud de vehículo integrado (IVHM) a cargo de monitorizar y determinar cuándo se produce una falla, el sistema 100 puede usar, ventajosamente, herramientas y recursos del sistema de IVHM para adquirir firmas presentes. En particular, los sensores de IVHM, tales como sensor de temperatura, sensor de vibración, sensores eléctricos pueden medir características físicas actuales. Puede ser necesario convertir las firmas presentes a un formato apropiado para permitir que una unidad 180 de comprobación del sistema 100 compare de manera secuencial la firma presente con la firma almacenada correspondiente para cada componente. Si, como resultado de la comparación, las firmas son válidas, la unidad 180 de comprobación autentifica el primer componente 102. Una comparación puede resultar satisfactoria incluso si las firmas no son idénticas, pero se encuentran dentro de un intervalo previsto tal como se explicará a continuación. Cuando todos los componentes 102 críticos se autentifican de manera válida, se considera que el propio aparato 110 está autentificado.

La situación anterior muestra que el caso de autentificación se inició por la situación de permitir una determinada función del aparato 110. No obstante, también se contempla que la autentificación puede realizarse en base a un intervalo de tiempo para garantizar de manera constante la integridad del aparato 110.

La figura 2A muestra un aparato 200 esquemático que consiste en cuatro componentes marcados como S1, S2, S3 y S4. Teniendo en consideración un componente S5 malicioso añadido al aparato 200, tal como se ilustra por la figura 2B. Como consecuencia, uno o más de los componentes S1-S4 pueden verse comprometidos y el propio aparato 200. Esto puede conducir a un mal funcionamiento, toma de control, u otras acciones inesperadas o maliciosas.

Cuando se aplican medidas de seguridad de nivel superior convencionales, tales como, por ejemplo, autentificación basada en IFF, la autentificación puede permanecer positiva, aunque la misión pueda verse comprometida con consecuencias impredecibles.

Por ejemplo, si el aparato 200 es un vehículo aéreo no tripulado (UAV) y se toma el control de un componente crítico, puede hacerse que el UAV aterrice en una base maliciosa en lugar de en una base propia.

Para tratar estos problemas de seguridad, se proponen varias medidas alternativas. En primer lugar, los componentes críticos necesitan diferenciarse tal como se menciona cuando se comenta la figura 1. Tales componentes críticos pueden ser aquellos que, si se ven comprometidos, puedan activar una falla general. Por tanto, es aconsejable que se monitoricen y autentifiquen de manera continua. Esto significa intercambiar información relevante entre componentes interdependientes en la trayectoria de autentificación, por ejemplo, la plataforma y

cámaras integradas.

En general, los procedimientos de seguridad iniciales incluyen las siguientes subtareas secuenciales: identificación, autentificación y autorización. Teniendo en cuenta la situación de UAS, la autorización forma parte de un sistema de gestión de misión (MMS) y depende por completo de la correcta identificación y autentificación previas. Por tanto, las técnicas propuestas en el presente documento se centran, principalmente, en la mejora de las dos subtareas anteriores: identificación y autentificación. Estas subtareas implican actualmente una intervención humana muy frecuente. En su lugar, la presente divulgación propone un enfoque entre máquinas (M2M) que evita cualquier requisito de implicación humana. Para ese fin, se describe una identificación/autentificación de UAS secuencial en más detalle a continuación.

La integridad de una misión de UAS depende de una identificación y autentificación con éxito del UAV en la unidad de orden y control (C2). La unidad de C2 necesita tener un acceso exclusivo a y un control sobre los UAV, lo que incluye componentes críticos, como cargas útiles operativas integradas y subsistemas (cámaras, sensores, accionadores, antenas, enlaces de datos, etc.). Una integridad completa de componentes críticos de UAV es una condición para la seguridad, soberanía y ejecución con éxito de la misión. En esta divulgación, se define soberanía como un control completo e independiente sobre un aparato.

La figura 3A muestra un ejemplo de una red de dependencias de autentificación. Unos primeros puntos de nodo con respecto a un segundo nodo y flechas indican la dependencia a un componente. Un componente se considera validado cuando todos los nodos en la trayectoria de dependencia ya están validados. Por consiguiente, la validación en esta red debe seguir un orden específico para cumplir la autentificación global. A este respecto, la figura 3B muestra un diagrama de componentes que muestra primeras dependencias próximas a dos nodos a modo de ejemplo en la red.

En más detalle, la figura 3A se refiere a un UAS alimentado con batería, que incluye un ordenador 310 a bordo que envía señales a un controlador 312, que ajusta la alimentación eléctrica a la central eléctrica. Las órdenes procedentes de una estación en tierra (no mostrada) se envían al ordenador 310 a bordo desde un receptor 302. El ordenador 310 a bordo se alimenta a partir de una batería 308 principal, colocada en un recipiente 306 de seguridad (para mitigar el impacto de posible sobrecalentamiento de batería y reacción de inestabilidad térmica). Este ordenador 310 a bordo también controla un ventilador 304 de enfriamiento usado para regular la temperatura de un transpondedor 314 de IFF y la batería 308 restante.

En este caso particular, con el fin de autentificar el controlador 312 y el transpondedor 314 de IFF, requisitos mínimos (obtenidos de una lista de dependencias usando una base de datos de configuración) deben autentificar el ordenador 310 a bordo y el ventilador 304 de enfriamiento, respectivamente. El propio ordenador 310 a bordo facilita la autentificación de firma digital. El ventilador 304 de enfriamiento puede autentificarse usando sus características físicas, por ejemplo, velocidad de rotación de ventilador y la firma de vibraciones resultante. Por tanto, es necesario un sensor adecuado para medir su firma física actual. Dado que un UAV incluye normalmente muchos sensores integrados, deben usarse para obtener las firmas físicas necesarias.

La siguiente secuencia de relaciones de autentificación jerárquicas se representa en la figura 3A y 3B:

- la autentificación del ordenador 310 a bordo depende de la autentificación del receptor 302 y la batería 308 principal;

- la autentificación del controlador 312 depende de la autentificación del ordenador 310 a bordo;

No es necesario comentar que la red de dependencias de autentificación puede ampliarse según sea necesario. Por ejemplo, las cadenas de autentificación pueden ampliarse a otros componentes en la trayectoria de dependencia. Por ejemplo, la relación de autentificación para el controlador 312 puede incluir no solo el ordenador 310 a bordo, sino también el receptor 302. De manera similar, las trayectorias adicionales pueden incluirse para unir el transpondedor 314 de IFF al ordenador 310 a bordo y al receptor 302. Además de la situación de UAS, que se tiene en consideración, este modelo de dependencia también puede aplicarse a muchas otras realizaciones.

La figura 4 señala varias firmas físicas y digitales que pueden ser eficaces en cualquier autentificación del propio aparato o solo un determinado único componente. En cualquier caso, cada componente del aparato que se somete a la autentificación debe tener una o más firmas que pueden ser o bien físicas 408 o bien digitales 404 o ambas. Las firmas 404 digitales pueden ser un ID de procedimiento, una tarjeta 404 inteligente o RFID 406. Las firmas 408 físicas se refieren a características que identifican de manera única al componente. Por ejemplo, computacional 410, aerodinámica 412, eléctrica 414, mecánica 416, tal como: firma de vibración mecánica, volumen, forma, albedo, patrón de consumo de energía, firma eléctrica, firma magnética, firma de radiofrecuencia o cualquier combinación de las mismas. Puede ser necesario convertir estas firmas a un formato uniforme, y almacenarlas en una base de datos de configuración integrada.

El procesamiento digital autentificación de firmas es directo y un algoritmo previsto puede admitir, o no, determinadas desviaciones de valores de firmas almacenados, para tener en consideración posibles inexactitudes de mediciones de datos físicos o fallos de transferencia. Por ejemplo, la ausencia de una de las validaciones

digitales puede considerarse aceptable. La relajación de las condiciones depende de circunstancias. Véanse a continuación algunos casos.

En relación a la validación de firma física, siempre existen determinadas desviaciones. La solución propuesta puede requerir admitir un determinado intervalo de valores exactos previstos, para tener en consideración variaciones inevitables en el entorno físico, por ejemplo, variación de temperatura, cambios de condición límite (en tierra o durante el vuelo), etc. Si existen k posibles parámetros de validación independientes para autentificar un componente del aparato, estos parámetros de validación definen un espacio de firmas “maquinométrico”. Este concepto se ilustra en la figura 5.

La figura 5 muestra gráficamente un espacio 500 tridimensional constituido por las siguientes firmas físicas para un UAV dado: primera frecuencia modal de un subsistema f(Hz) seleccionado, el periodo de retardo en la elevación de corriente tras aplicar una etapa entrada de empuje t1 y un retardo de tiempo en cabeceo de fuselaje tras aplicar una entrada escalonada al elevador t2.

Para mejorar la robustez, tal como se comentó anteriormente, se definen intervalos de confianza válidos para los valores de firmas previstos. Si los valores se encuentran dentro de determinados intervalos, la firma puede ser válida. Por ejemplo, tal como se representa en el paralelepípedo 502 de la figura 5: 2,0 Hz < f(Hz) < 4,5 Hz, 0,1 s < t1 < 0,6 s y 0,5 s < t2 < 0,7 s. Por tanto, el UAV se autentifica con éxito si los parámetros obtenidos se encuentran dentro de estos intervalos.

La figura 6 muestra un diagrama de flujo simplificado de diversas operaciones realizadas para autentificar un aparato según un ejemplo. El diagrama de flujo incluye una etapa 602 de recuperación a partir de una base 604 de datos de configuración para obtener un conjunto de n componentes críticos del aparato que necesita autentificarse. Entonces una etapa 606 de construcción construye una lista de dependencias para los n componentes críticos. Una vez preparada la lista de dependencias, un bucle discurre n veces y realiza una etapa 610 de selección para tomar un elemento de la lista de dependencias. Este elemento se procesa y verifica según un procedimiento 612 de autentificación de múltiples factores. La autentificación de múltiples factores se realiza en bucle sobre todas las dimensiones del espacio de firmas (factores) “maquinométricos”. El procedimiento 612 de autentificación de múltiples factores para cada componente individual se representa en la figura 7. Cada vez que el resultado de la etapa 614 de comprobación para el elemento dado sea positivo, el componente se autentifica. Una vez que la etapa 608 de comprobación indica que la lista de dependencias está vacía, la autentificación de aparato es positiva. Obsérvese que la autentificación falla cuando se considera un primer componente crítico “no autentificado.”

La figura 7 muestra una autentificación 612 de bajo nivel en otro diagrama de flujo simplificado. Esto es un bucle interno dentro del procedimiento representado en la figura 6. Un componente se autentifica con factor k, cuando cada una de las k firmas asociadas con el componente crítico dado se comprueba de manera válida. Un componente que tiene k firmas necesita pasar la etapa 702 de validación k veces. Cada vez que se valida una firma, la siguiente se procesa hasta que se comprueba 704 que no hay más firmas asociadas con ese componente (o alternativamente que existe un resultado de “no autentificado”). Por tanto, la autentificación del componente 706 es positiva siempre y cuando se comprueben de manera válida k firmas. Este procedimiento de autentificación a nivel de componente debe realizarse para un único componente o bien periódicamente o bien de manera asíncrona (por ejemplo, siempre que se añada un nuevo componente).

Si el aparato es un UAV 300, la adición de un nuevo componente requiere la actualización de la base 604 de datos de configuración. Esto puede lograrse a través de un procedimiento automático, o solicitarse directamente por la unidad de comando y control (C2). La pérdida de autentificación para uno o más componentes críticos da como resultado una pérdida global de autentificación. Esa situación puede activar, de manera automática, acciones de contingencia de seguridad predefinidas. Estas acciones pueden incluir intercambio de información con la unidad de C2, llevar a cabo un procedimiento de reautentificación, volver a la base principal, interrumpir tareas de vuelo/misión, destrucción del UAV 300, etc. La manera de proceder con el aparato tras el fallo de autentificación no se encuentra dentro del alcance de esta presente divulgación.

La figura 8 muestra una arquitectura de transmisión de datos para la implementación de las presentes enseñanzas en un UAV 300. Una de las piezas clave de esta arquitectura es un módulo 810 de autentificación. Este módulo 810 de autentificación monitoriza cambios físicos y se correlaciona con cualquier cambio de identidad dado que está relacionado con una base 806 de datos de vuelo/misión. El módulo 810 de autentificación ejecuta tareas de identificación y autentificación para cada componente crítico. Existe una correspondencia de esta arquitectura con el diagrama de bloques de la figura 1. El módulo 810 de autentificación es una posible implementación de SW para un UAV de la unidad 120 de recuperación y la unidad 180 de comprobación. La base 806 de datos de vuelo/misión también almacena la información de autentificación para componentes de UAV tal como la base 140 de datos de configuración.

Cada componente del UAV considerado crítico se somete a una autentificación individual, aquellos menos críticos pueden requerir solamente una simple autentificación basada en certificación, al tiempo que aquellos considerados esenciales pueden requerir una autentificación de múltiples factores tal como se comentó anteriormente. El módulo 810 de autentificación está a cargo de evaluar el estado de autentificación. Dependiendo de la situación, puede o

bien garantizar o bien denegar una autentificación positiva o enviar una recomendación relevante a la unidad de C2.

La mayor parte de los UAV están equipados con un bus 818 digital para facilitar el intercambio de datos entre diversos componentes (por ejemplo, aviónica y sensores). El intercambio de datos seguro a través del bus 818 digital requiere aplicar un procedimiento de seguridad de tres etapas completo (identificación, autentificación, autorización) proporcionado por el módulo 810 de autentificación. Los datos enviados a través de este bus 818 pueden monitorizarse de manera continua mediante el módulo 810 de autentificación para detectar y autentificar cualquier nuevo componente conectado al bus 818. Los requisitos de seguridad implican que la identidad pueda validarse cada vez que el UAV envía/recibe datos a través del bus 818 (de manera similar a las denominaciones en el ARINC 429 habitual y enlaces virtuales en la especificación de ARINC 664, parte 7).

En algunos casos, una comunicación de extremo a extremo necesita algunos módulos adicionales para mediar o completar la comunicación. Los módulos pueden observarse como un único componente o como un grupo de componentes, es decir, un subsistema, que se autentifica en conjunto. Uno de los beneficios de la presente arquitectura es la capacidad de autentificar datos a partir de fuentes ya identificadas positivamente. Tal como se representa en la figura 8, un módulo 802 A redacta datos en el bus 818, y el módulo 804 B lee estos datos junto con datos de vuelo procedentes de una base 806 de datos de vuelo que pasó con éxito los procedimientos de identificación y autentificación. Los agentes 812, 816, 814 de autentificación son preferiblemente aplicaciones de software generadas y distribuidas de manera automática por el módulo 810 de autentificación para gestionar las tareas de autentificación principales y para mediar entre el bus 818 digital y un módulo en cuestión. Los agentes 812, 816, 814 de autentificación sirven. El papel de los agentes 812, 814, 816 de autentificación se describe a continuación. Los agentes de autentificación comprueban la integridad del módulo, pasan la información de autentificación al módulo de autentificación y controlan la entrada/salida del módulo correspondiente.

La arquitectura de la figura 8 permite insertar una autorización dinámica entre la capa de datos (bus 818) y la capa de aplicación (módulo 802 A, módulo 804 B y fuentes de datos tal como la base 806 de datos de misión y vuelo). Si uno de los módulos no se identifica o autentifica (o incluso no se autoriza), un agente 812, 816, 814 asociado notifica al módulo 810 de autentificación de que puede desconectar el módulo no identificado del bus 818, o reducir el nivel de confianza que sigue el modelo de confianza ya definido, dependiendo del nivel de importancia de tal funcionalidad de módulo. El modelo de confianza definido por usuario es necesario para la cooperación de agentes de seguridad.

El nivel de confianza, el estado de identificación o autentificación, para cada componente del UAV 300 puede solicitarse desde una tabla proxy construida a partir de la base 806 de datos de vuelo. Esta tabla proxy contiene el estado de autentificación actualizado de todos los componentes. Sus datos son públicos y accesibles para todos los agentes 812, 816, 814 de autentificación. Si un módulo 810 de autentificación decide denegar la autentificación a un módulo, el estado de este módulo en la tabla proxy se actualiza y el agente correspondiente actúa en consecuencia. Cada agente 812, 816, 814 de autentificación lee la tabla proxy antes de la acción de denegación/aceptación de los datos en cuestión en el bus 818. Se observa que muchos detalles de implementación pueden variar dependiendo de los requisitos de arquitectura o recursos. Por ejemplo, el agente de autentificación puede solo someter a prueba la integridad del módulo e informar al módulo de autentificación sobre los resultados, o someter a prueba y llevar a cabo cualquier acción sobre la que el módulo autentificación tomaría su decisión.

La figura 9 presenta otra realización a modo de ejemplo del sistema 100 para un UAS que incluye el UAV 924 y estación 922 de control en tierra. Las firmas digital y física usadas para la autentificación de componentes específicos se muestran en líneas discontinuas delgadas, usando cursiva. La trayectoria de autentificación del sistema 100 se muestra en líneas discontinuas en negrita. En esta realización particular, el sistema 100 forma parte del ordenador a bordo principal del UAV 924. La autentificación de múltiples factores se indica con una C en mayúsculas dentro de un círculo.

La autentificación del motor 904 se realiza usando firmas físicas. En particular, firmas eléctricas (resistencia (R) y corriente (I)) y también temperatura (T), para un modo de vuelo dado. La autentificación del ordenador 920 a bordo se realiza usando una firma física y una digital, (identificación digital por ordenador y tensión eléctrica por ordenador). Para el motor 904 y otros componentes, también puede usarse cualquier característica de software de control relevante para la autentificación de múltiples factores.

El UAV 924 recibe una entrada de misión a partir de la estación 922 de control en tierra. El ordenador 920 a bordo procesa la entrada de misión, realiza tareas que dependen de esa entrada (tal como control de cámara o tareas de navegación particulares) y ejecuta tareas de manera independiente de la entrada procedente de la estación de control en tierra, tal como detección y evasión de obstáculos.

Asúmase que, para una misión determinada, la autentificación del UAV 924 requeriría la autentificación de un motor 904 como uno de los componentes críticos. El procedimiento de autentificación relacionado sería uno habitual basándose en el enfoque “maquinométrico” dado a conocer. La autentificación del motor 904 no solo requiere la autentificación de sus firmas físicas a través de la comprobación de si se encuentran dentro de los intervalos previstos para la resistencia eléctrica, R, un intervalo para la corriente, I, y un intervalo para la temperatura, T, sino que también depende de la autentificación positiva de componentes próximos: la unidad 916 de control de motor y el

propulsor 902. El agente de autentificación de software compara la firma digital de la unidad 916 de control de motor frente a la información de autentificación almacenada en la tabla proxy. Esta puede ser, por ejemplo, información relacionada con la temporización de la secuencia de energización de bobina de estator. La información de paso/fallo con respecto a la autentificación de unidad 916 de control de motor se pasa, entonces, al módulo 918 de autentificación. Obsérvese que el procedimiento de autentificación de la unidad 916 de control de motor puede ampliare adicionalmente a través de, por ejemplo, la comprobación de su firma térmica. De manera similar, la información sobre la firma acústica del propulsor correspondiente a la entrada de energía compatible con la firma del controlador 916, se pasa al módulo 918 de autentificación. Solo si se pasan todas las etapas de autentificación, el módulo 918 de autentificación considera que el motor 904 está autentificado. Si no, el módulo 918 de autentificación actúa de manera acorde. Por ejemplo, puede ordenar que el agente de autentificación modifique la operación de la unidad 916 de control de motor, de modo que se reduce el suministro de energía al motor y se fuerza al UAV 924 a que aterrice. De manera similar, la trayectoria de dependencia de la cámara 906 incluye el servosistema que incluye un servo 910 de giro y un servo 910 de inclinación, y el ordenador 920 a bordo. Tanto el ordenador como la camera necesitan autentificarse a través de la autentificación de múltiples factores.

Estas y otras características, funciones, y ventajas que se han comentado pueden lograrse de manera independiente en diversas realizaciones o pueden combinarse en incluso otras realizaciones.

REIVINDICACIONES

1. Método entre máquinas de autentificación de múltiples factores que comprende las etapas de:

i) identificar al menos un componente (102) crítico de un aparato (110) en respuesta a una solicitud de autentificación para el aparato (110);

ii) recuperar información de autentificación para el componente (102) crítico, en el que la información de autentificación comprende una pluralidad de firmas físicas y digitales previstas como factores de autentificación para el componente (102) crítico y al menos un componente (104) adicional asociado con el componente (102) crítico, mediante lo que las firmas físicas previstas se relacionan con características de comportamiento o físicas que se identifican únicamente con el componente (102,104) adicional o crítico respectivo;

iii) adquirir firmas físicas presentes mediante medición y firmas digitales para el componente (102) crítico y el al menos un componente (104) adicional asociado con las mismas; y

iv) para cada componente (102,104) adicional y crítico, comprobar la validez de cada firma física y digital presente con la firma física y digital previstas correspondientes y autentificar el aparato (110) si las firmas físicas y digitales para cada componente (102,104) adicional y crítico son válidas.

2. Método de autentificación de múltiples factores según la reivindicación 1, en el que la información de autentificación para el componente (102) crítico comprende una lista de dependencias con una secuencia de componentes (104) adicionales asociada con el componente (102) crítico para comprobarse de manera secuencial.

3. Método de autentificación de múltiples factores según la reivindicación 1 ó 2, en el que la identificación del componente (102) crítico depende de la función que va a realizarse por el aparato (110).

4. Método de autentificación de múltiples factores según cualquiera de las reivindicaciones 1 a 3, en el que, tras producirse una situación en el aparato (110), se activa una solicitud de autentificación.

5. Método de autentificación de múltiples factores según cualquiera de las reivindicaciones 1 a 4, en el que la solicitud de autentificación para el aparato (110) se activa de manera periódica.

6. Método de autentificación de múltiples factores según cualquiera de las reivindicaciones 1 a 5, en el que las firmas físicas de componentes (102, 104) adicionales y críticos se adquieren a partir de mediciones de sensores del aparato (110).

7. Método de autentificación de múltiples factores según cualquiera de las reivindicaciones 1 a 6, en el que una o más firmas de componentes (102,104) adicionales y críticos se adquieren comunicándose con un sistema de gestión de salud de vehículo integrado que monitoriza el aparato (110).

8. Método de autentificación de múltiples factores según cualquiera de las reivindicaciones 1 a 7, en el que las firmas físicas de componentes (102,104) adicionales y críticos se convierten en un formato digital que va a almacenarse o a comprobarse.

9. Método de autentificación de múltiples factores según cualquiera de las reivindicaciones 1 a 8, en el que una firma digital o física presente es válida cuando se encuentra dentro de un intervalo predefinido de las firmas digital o física previstas correspondientes.

10. Sistema para autentificación de múltiples factores entre máquinas de un aparato (110) que comprende:

i) una unidad (120) de recuperación configurada para identificar al menos un componente (102) crítico de un aparato (110) en respuesta a una solicitud de autentificación para el aparato (110), estando la unidad (120) de recuperación configurada además para recuperar información de autentificación para el componente (102) crítico, en el que la información de autentificación comprende una pluralidad de firmas físicas y digitales previstas como factores de autentificación para el componente (102) crítico y al menos un componente (104) adicional asociado con las mismas, mediante lo que las firmas físicas previstas se relacionan con características de comportamiento o físicas que solamente identifican el componente (102,104) adicional o crítico respectivo;

ii) una unidad (160) de adquisición configurada para adquirir firmas físicas presentes mediante medición y firmas digitales para el componente (102) crítico y el al menos un componente (104) adicional; y

iii) para cada componente (102,104) adicional y crítico, una unidad (180) de comprobación configurada para comprobar la validez de cada firma física y digital presente con la firma física y digital prevista correspondiente, estando la unidad (180) de comprobación configurada además para autentificar el aparato (110) si las firmas física y digital para cada componente (102,104) adicional y crítico son válidas.

11. Sistema según la reivindicación 10, que comprende además una base (140) de datos de configuración para almacenar firmas físicas y digitales previstas de componentes (102, 104) del aparato (110).

12. Sistema según la reivindicación 10 u 11, que comprende además sensores para medir firmas físicas de componentes (102, 104) adicionales y críticos del aparato (110).

13. Sistema según cualquiera de las reivindicaciones 10 u 11, en el que la unidad (160) de adquisición está configurada para adquirir firmas físicas de componentes (102, 104) adicionales y críticos a partir de sensores del aparato (110).

14. Sistema según cualquiera de las reivindicaciones 10 u 11, en el que la unidad (160) de adquisición está configurada para comunicarse con un sistema de gestión de salud de vehículo integrado que monitoriza el aparato (110) para adquirir firmas digitales o físicas.

15. Producto de programa informático para la autentificación entre máquinas de un aparato, que comprende instrucciones de código informático que, cuando se ejecutan por un procesador, provocan que el procesador realice el método según cualquiera de las reivindicaciones 1 a 9.

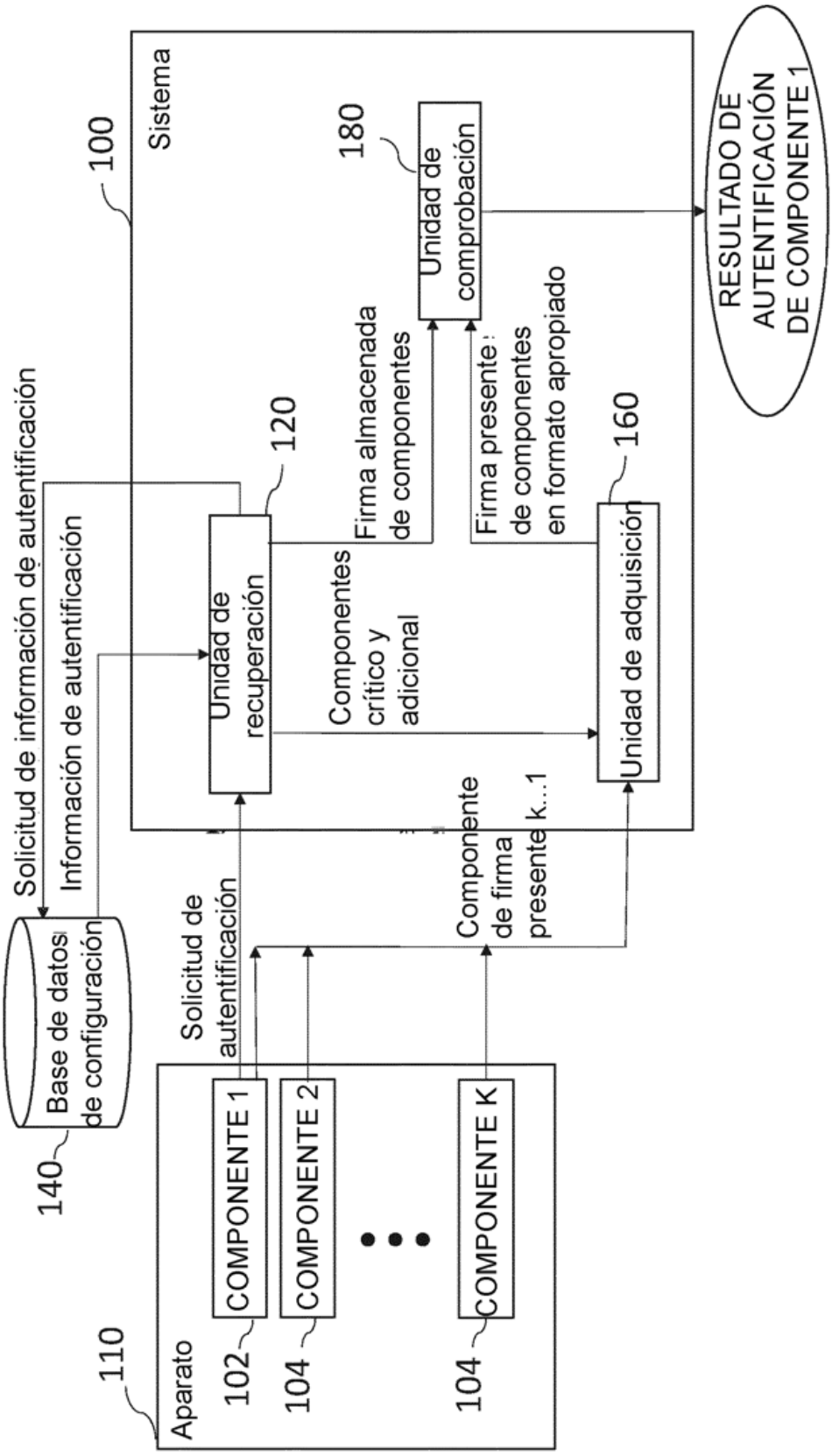
Sistema
100
180
Unidad de comprobación
RESULTADO DE AUTENTIFICACIÓN DE COMPONENTE 1
Firma almacenada de componentes
Firma presente de componentes en formato apropiado
120
160
Unidad de recuperación
Unidad de adquisición
Componentes crítico y adicional
Solicitud de información de autentificación
Información de autentificación
Base de datos de configuración
140
Solicitud de autentificación
Componente de firma presente k...1
Aparato
110
COMPONENTE 1
COMPONENTE 2
COMPONENTE K
102
104
104

Fig. 1

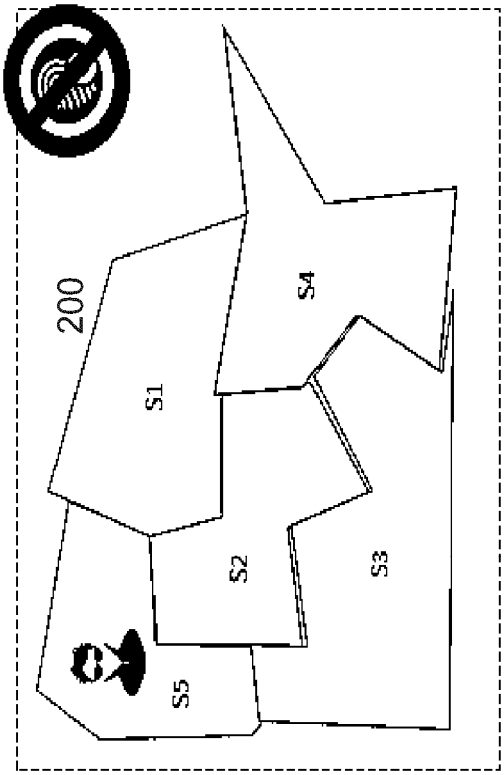

Fig. 2B

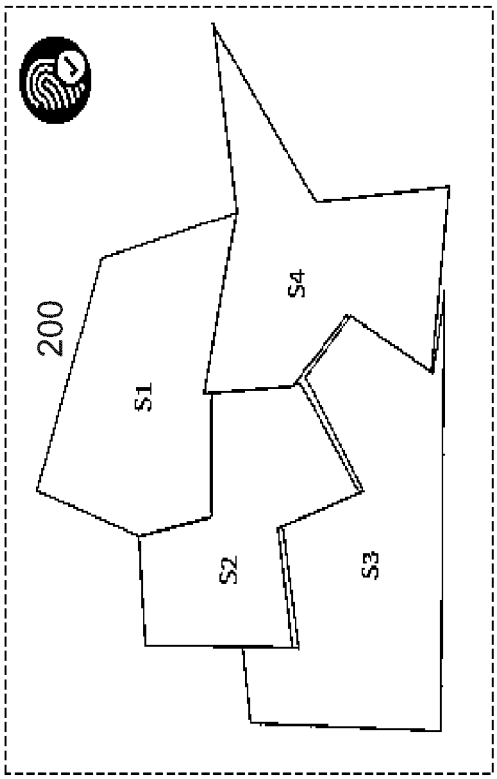

Fig. 2A

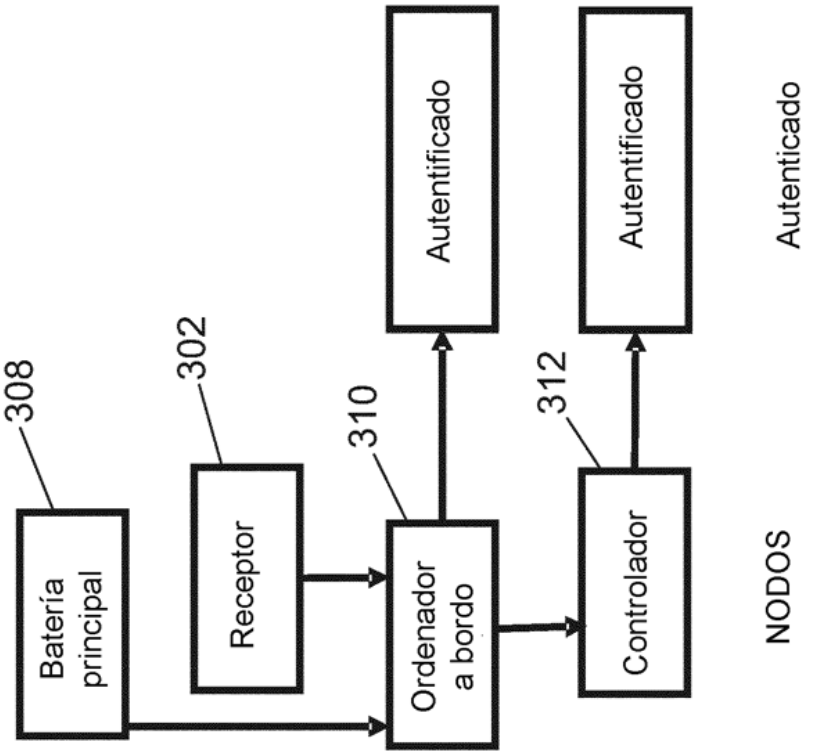
Batería principal
308
Receptor
302
Ordenador a bordo
310
Controlador
312
Autentificado
Autentificado
NODOS
Autenticado

Fig. 3B

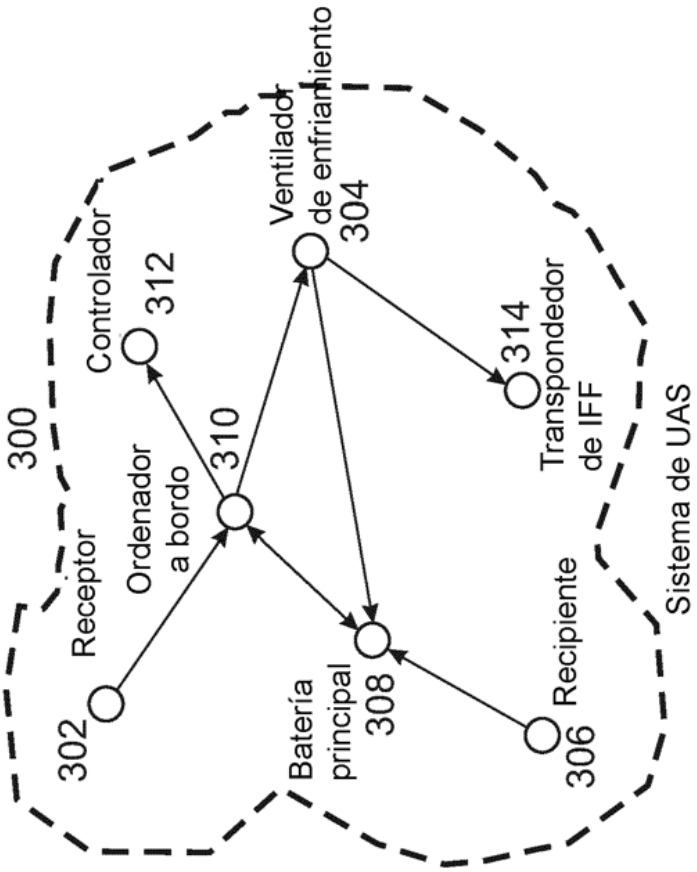
300
Receptor
302
Ordenador a bordo
310
Controlador
312
Ventilador de enfriamiento
304
Transpondedor de IFF
314
Batería principal
308
Recipiente
306
Sistema de UAS

Fig. 3A

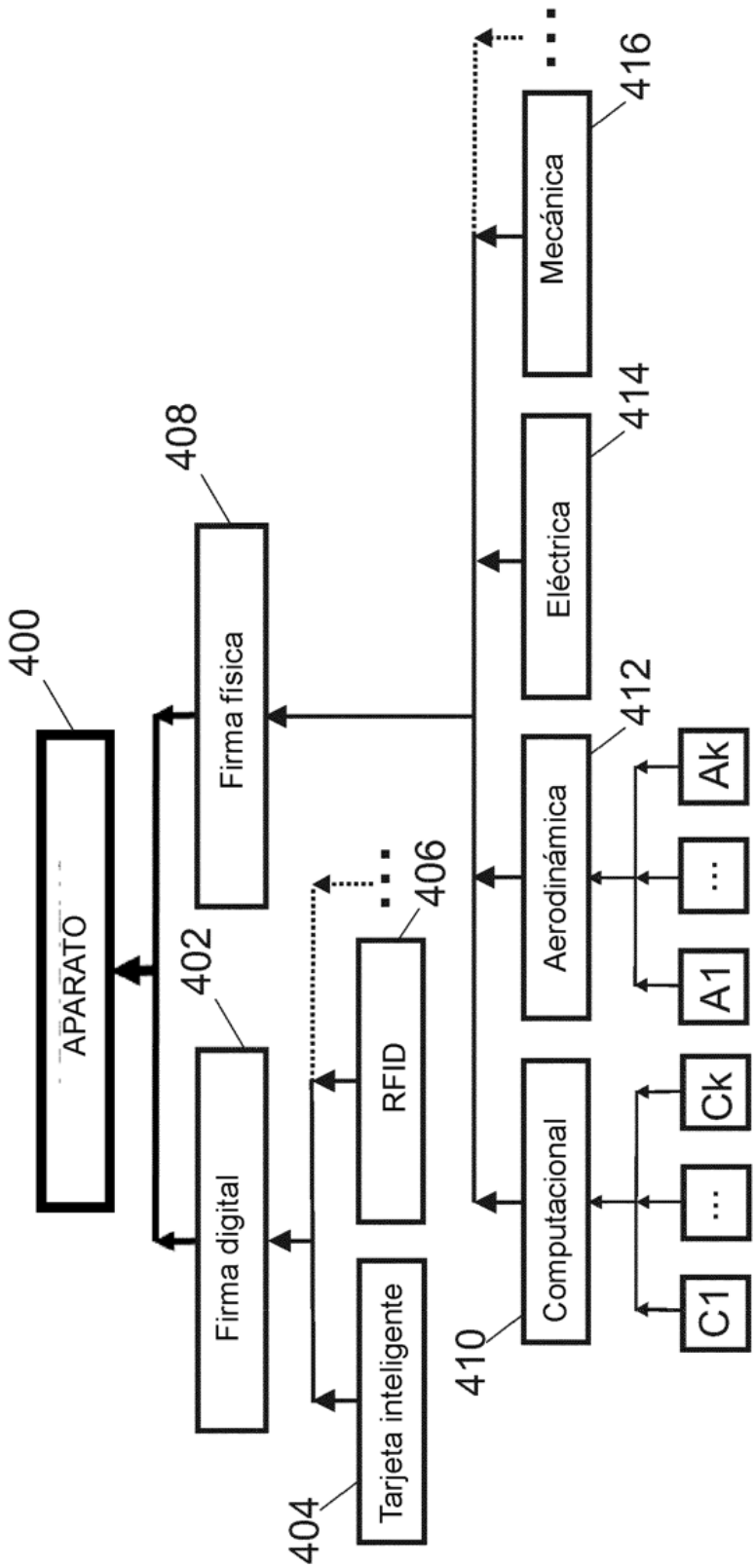
400
APARATO
402
Firma digital
404
Tarjeta inteligente
406
RFID
408
Firma física
410
Computacional
C1
...
Ck
412
Aerodinámica
A1
...
Ak
414
Eléctrica
416
Mecánica
...

Fig. 4

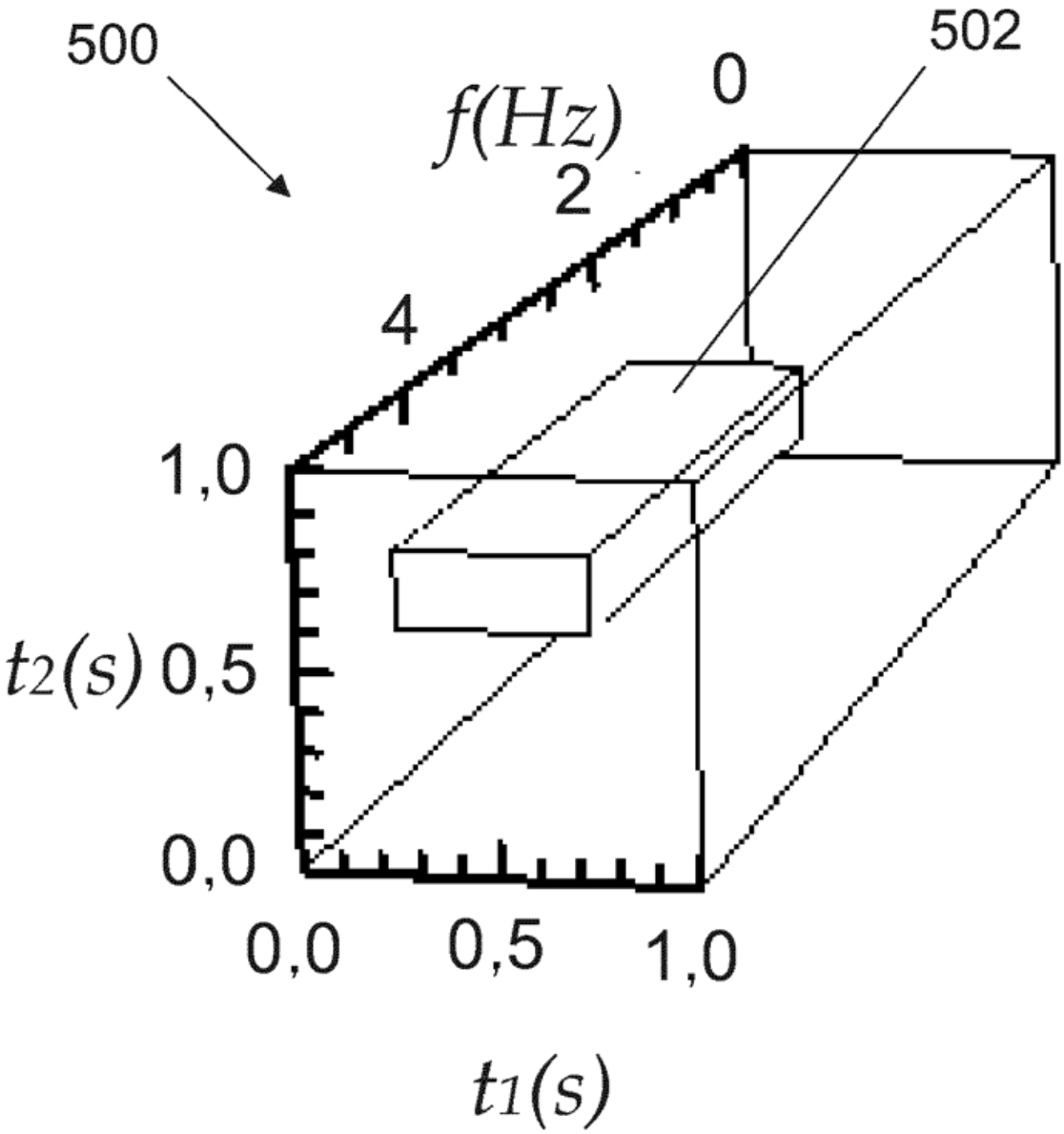

Fig. 5

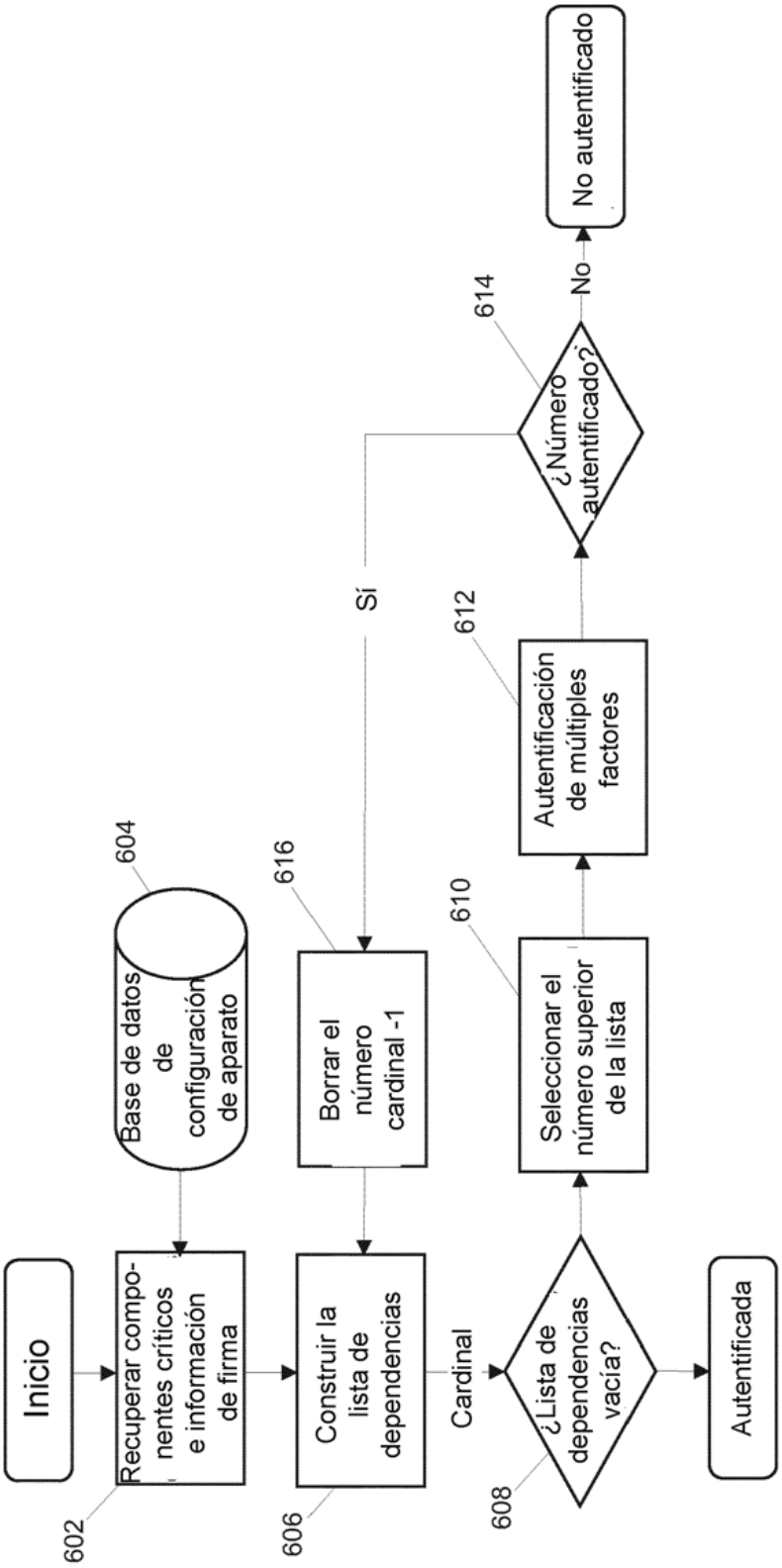
Inicio
Recuperar componentes críticos e información de firma
602
Base de datos de configuración de aparato
604
Construir la lista de dependencias
606
Borrar el número cardinal -1
616
Cardinal
¿Lista de dependencias vacía?
608
Sí
Seleccionar el número superior de la lista
610
Autentificación de múltiples factores
612
¿Número autentificado?
614
No
No autentificado
Autentificada

Fig. 6

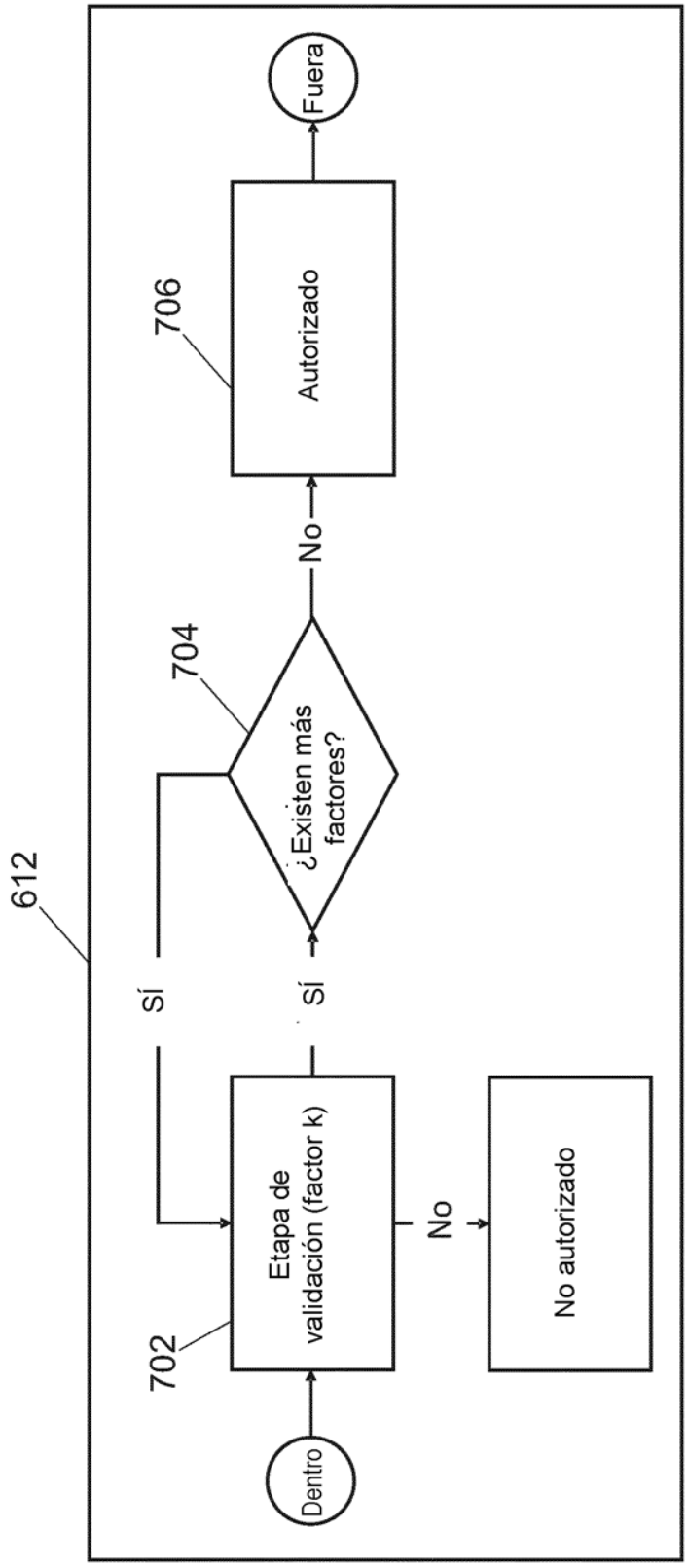
612
Dentro
Etapa de validación (factor k)
702
No
No autorizado
Sí
¿Existen más factores?
704
Sí
No
Autorizado
706
Fuera

Fig. 7

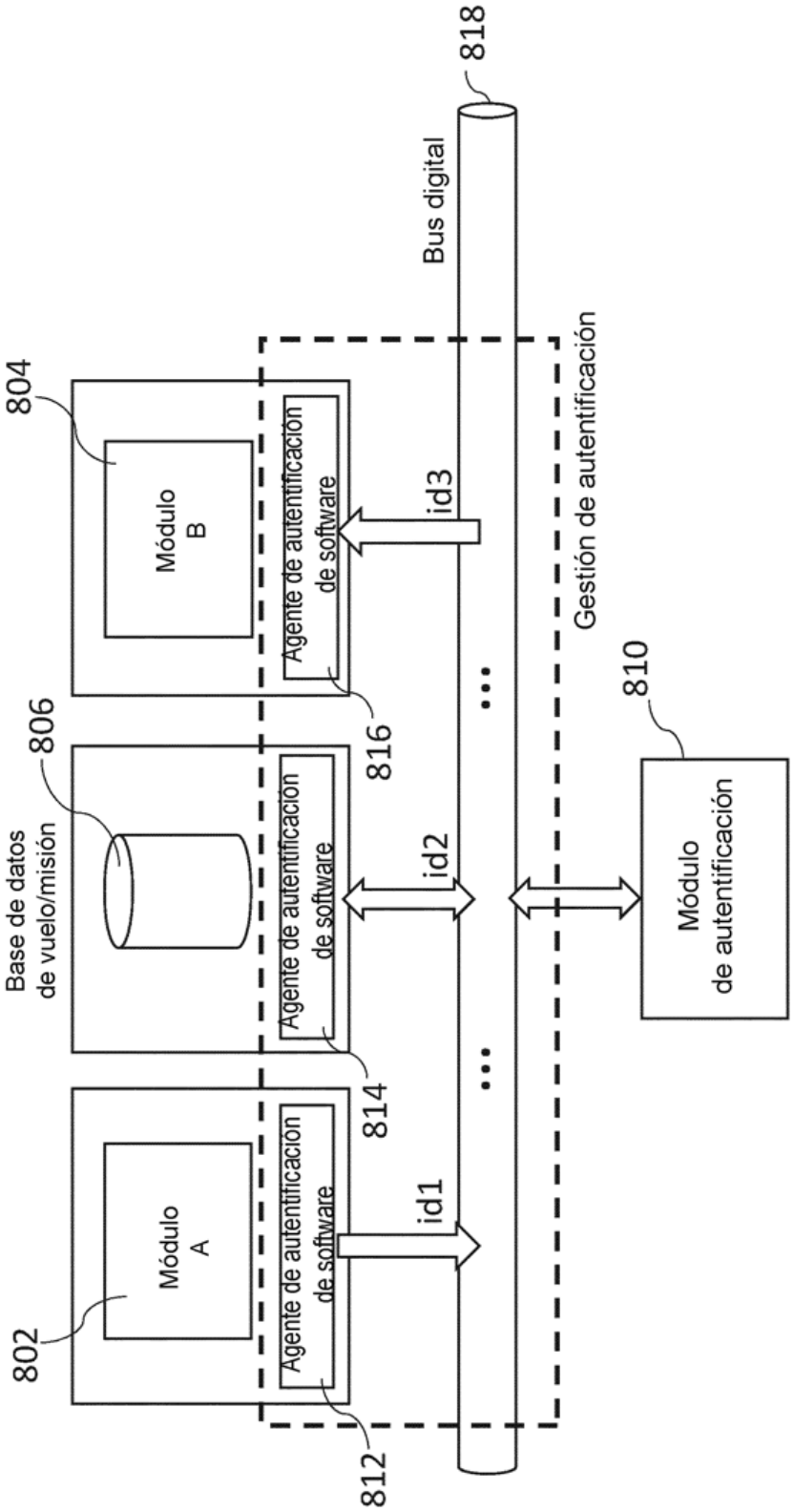
818
Bus digital
804
Módulo
B
Agente de autentificación
de software
id3
816
Gestión de autentificación
810
806
Base de datos
de vuelo/misión
Agente de autentificación
de software
id2
Módulo
de autentificación
814
Módulo
A
Agente de autentificacion
de software
id1
802
812

Fig. 8

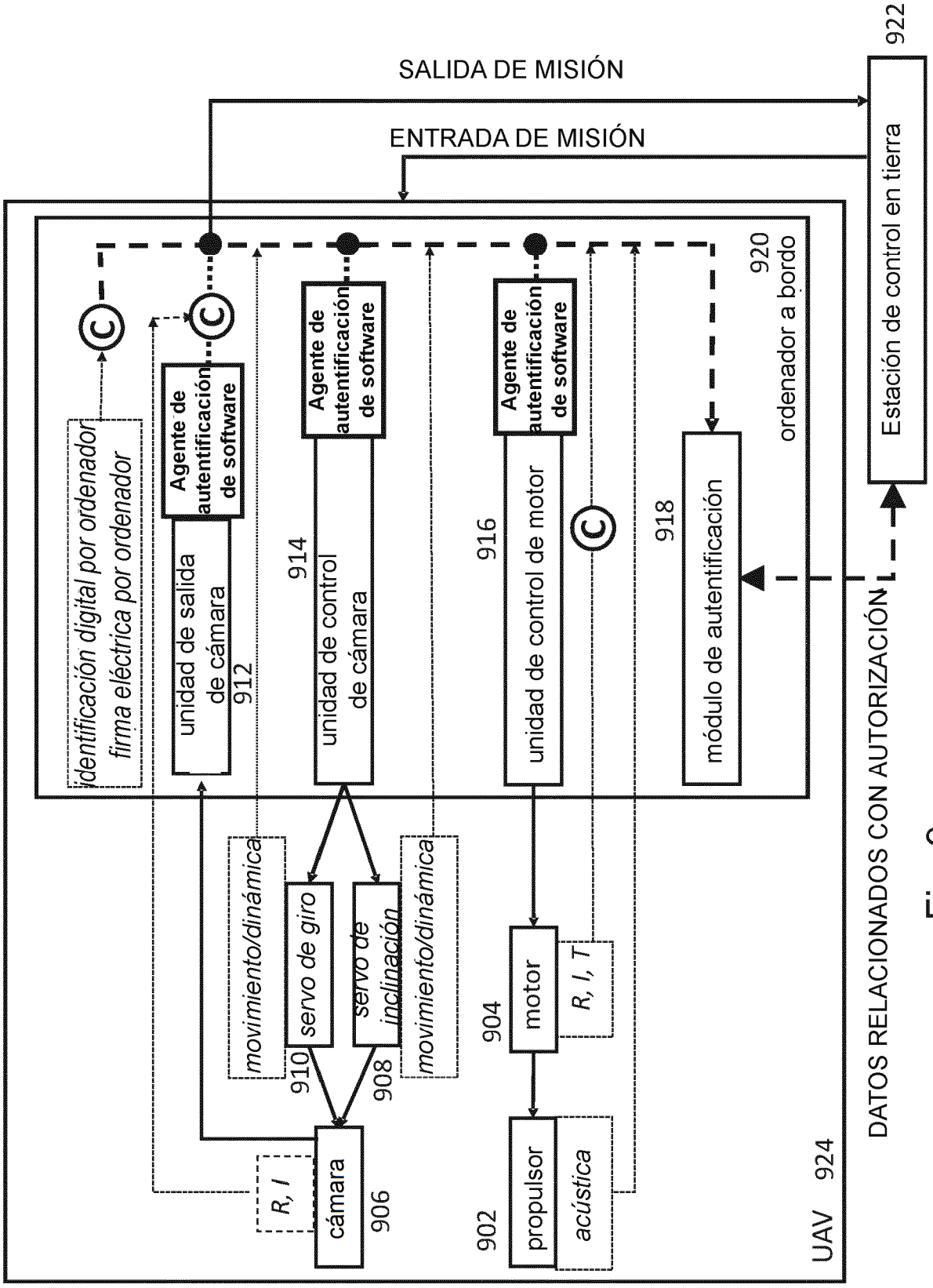
SALIDA DE MISIÓN
ENTRADA DE MISIÓN
922
Estación de control en tierra
DATOS RELACIONADOS CON AUTORIZACIÓN
920
ordenador a bordo
identificación digital por ordenador
firma eléctrica por ordenador
Agente de autentificación de software
unidad de salida de cámara
912
Agente de autentificación de software
914
unidad de control de cámara
Agente de autentificación de software
916
unidad de control de motor
C
918
módulo de autentificación
movimiento/dinámica
servo de giro
910
servo de inclinación
908
movimiento/dinámica
R, I
cámara
906
902
propulsor
acústica
904
motor
R, I, T
UAV
924

Fig. 9