(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 387 459**

(51) Int. CI.:
G06F 11/00 (2006.01)
G06F 11/07 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **10730168 .1**
(96) Fecha de presentación: **05.07.2010**
(97) Número de publicación de la solicitud: **2353089**
(97) Fecha de publicación de la solicitud: **10.08.2011**

(54) Título: **Procedimiento para representar información relativa a seguridad en un dispositivo de presentación y dispositivo para aplicar el procedimiento**

(30) Prioridad:
06.07.2009 EP 09164672
09.03.2010 WO PCT/EP2010/052946

(45) Fecha de publicación de la mención BOPI:
24.09.2012

(45) Fecha de la publicación del folleto de la patente:
24.09.2012

(73) Titular/es:
Deuta-Werke GmbH
Paffrather Strasse 140
51465 Bergisch Gladbach, DE

(72) Inventor/es:
MANZ, Holger;
GANZ, Rudolf y
HAAS, Thorsten

(74) Agente/Representante:
Arpe Fernández, Manuel

DESCRIPCIÓN

Procedimiento para representar información relativa a seguridad en un dispositivo de presentación y dispositivo para aplicar el procedimiento.

[0001] La presente invención se refiere a un procedimiento para la representación o visualización en pantalla, en una forma segura, de información relevante para la seguridad, especialmente mediante la detección de errores críticos para la seguridad en el cálculo de la información a fin de generar datos de imagen que utilicen las siguientes etapas del procedimiento: introducción en un procesador de al menos un valor grabado de un parámetro de entrada, procesamiento mediante ordenador del parámetro de entrada, transformándolo en una secuencia de datos de imagen que representa el parámetro de entrada, transmitir la secuencia de datos de imagen a un dispositivo de presentación y la representación o visualización de dicha secuencia de imágenes en dicho dispositivo de presentación.

[0002] En la actualidad, cada vez se utilizan más las pantallas TFT como unidades de visualización en muchas aplicaciones, en sistemas de control y supervisión, por ejemplo. Además de este tipo de casos, las pantallas TFT se utilizan normalmente para visualizar información crítica para la seguridad en el ámbito del control ferroviario o el de la aeronáutica, por ejemplo. En general, este tipo de unidades están basadas en un microcontrolador o PC equipado con un software que se ejecuta en un sistema operativo.

[0003] Se considera que un fallo constituye un fallo crítico para la seguridad si el dispositivo de presentación tan sólo parece funcionar correctamente o parece presentar una información correcta (coherente), pero cuando en realidad no representa la información genuina (real) facilitada a la unidad de visualización, por ejemplo, no es la velocidad real del tren. El dispositivo de presentación tan sólo muestra un valor aparentemente correcto, pero sin embargo, el fallo no puede ser detectado como tal por el observador.

[0004] Los procedimientos y dispositivos existentes para la aplicación de los procedimientos comprenden un procesador que genera una secuencia de datos de imagen correspondiente al parámetro de entrada, por ejemplo, orientados a imágenes o vectores, a fin de mostrar en el dispositivo de presentación la secuencia de datos de imagen. El dispositivo de presentación puede tener cualquier diseño, por ejemplo, un monitor o TFT, siendo este último utilizado con frecuencia en la actualidad. Teniendo en cuenta que la presente invención es independiente del tipo de pantalla utilizado, puede estudiarse cualquier tecnología aplicable. La unidad de procesamiento se conecta al dispositivo de presentación (panel) a través de interfaces digitales corrientes como el LVDS.

[0005] El procedimiento de detección y el dispositivo conforme a la presente invención no incluyen el dispositivo de presentación, pero lo consideran en este contexto un sistema perfecto y por tanto sin fallos. Esto se basa en la suposición de que en las pantallas se da normalmente una tasa de fallos enormemente baja, especialmente en el caso de pantallas de cristal líquido y sobre todo en relación con aquellos errores que podrían afectar a la seguridad, como se ha definido anteriormente. No obstante, tiene una importancia decisiva el hecho de que el valor del parámetro de entrada grabado y procesado por el sistema se visualice correctamente en el dispositivo de presentación.

[0006] Los procedimientos y aparatos comunes para la aplicación de los procedimientos se basan en la suposición de que el fallo de un dispositivo de presentación da como resultado una imagen obviamente falsa, que resulta evidente para el observador. Los datos visualizados pueden ser de carácter no constante, o verse interrumpidos, o por ejemplo, pueden cambiar de color, puede cancelarse una figura o mostrarse en una forma distorsionada. Asimismo, hay que señalar que un fallo o error de la propia pantalla también tendrá como resultado una representación visiblemente errónea de los datos.

[0007] Los actuales procedimientos y dispositivos para la generación de datos digitales de imagen suelen tener una acusada tendencia al error, debido a su inherente complejidad. Pueden producirse errores en todas las etapas del cálculo, debidos, por ejemplo, a un microprocesador defectuoso. También pueden producirse en el controlador gráfico, en los módulos de memoria individuales, en la fuente de alimentación y también en la aplicación de software de visualización, pudiendo éstos últimos deberse incluso a errores en la biblioteca de software gráfico o en otras librerías de software utilizadas por la aplicación de software específica. Por lo tanto, una prueba o aprobación de seguridad para la certificación del sistema general resulta muy complejo y debe siempre comprender todos los componentes, el hardware, el firmware y todo el software utilizado, incluyendo el sistema operativo. A mayor abundamiento, cualquier actualización o modificación/alteración de los componentes del sistema, incluyendo el software, requiere una nueva certificación del sistema completo. En la práctica, dicho proceso resulta tedioso y muy costoso, aunque resulta estrictamente necesario con los procedimientos y dispositivos acordes con la técnica anterior.

[0008] Se conocen procedimientos de una naturaleza diferente para garantizar una visualización segura de los datos de la imagen gracias a las patentes DE 4332143 A y EP 0856792 A.

[0009] El objeto de la presente invención consiste en proporcionar un procedimiento mejorado para conseguir una representación fiable de la información relativa a seguridad en un dispositivo de presentación, y un dispositivo para

la aplicación de dicho procedimiento, evitando de este modo, en buena medida, las desventajas mencionadas anteriormente y permitiendo especialmente sustituir o modernizar con facilidad los componentes del sistema.

[0010] En la realización más sencilla de la presente invención, esta tarea se logra mediante las siguientes etapas: transmisión de la secuencia de datos de imagen a una unidad de prueba, realizando una prueba de seguridad mediante la generación por ordenador de un código de prueba (huella dactilar) correspondiente a la secuencia de datos de imagen, comprobando el código de comprobación con una serie – discreta – de códigos de referencia, asignando el código de referencia identificado mediante este proceso, al posible valor correspondiente del parámetro de entrada y comparándolo con el valor del parámetro de entrada. Preferiblemente, la prueba de comprobación de los códigos de comprobación con los códigos de referencia se efectúa como una etapa integrada en la unidad de comprobación, lo que significa que los códigos de referencia se encuentran integrados en la unidad de comprobación. No obstante, en una realización simplificada, esta evaluación también puede ser llevada a cabo en otro componente que comprenda los datos necesarios.

[0011] Resulta evidente, para cualquier persona versada en la materia, que la invención presenta un procedimiento muy eficaz y seguro para garantizar una representación fiable (segura) de información relacionada con la seguridad, especialmente mediante visualización basada en píxeles.

[0012] De este modo, la unidad de prueba genera un resultado de la prueba positivo o negativo para el inicio de una reacción destinada a seguridad. De este modo, la unidad de comprobación puede contener diversos códigos de referencia que sean contables y distintos - discretos – en forma de cuadro, por ejemplo, que sean característicos de cada aplicación. Asimismo, se asignará a cada código de referencia cada uno de los posibles valores del parámetro de entrada. Por ejemplo, si el procedimiento se aplica para el examen o la comprobación del valor visualizado en un velocímetro de un vagón automotor, los diversos códigos de referencia pueden representar diferentes velocidades, en incrementos de 1 km/h, por ejemplo.

[0013] Una vez calculado el código de verificación, la prueba de seguridad proporciona una comprobación en forma de “búsqueda”, para comparar el código de verificación con los códigos de referencia existentes. Si no puede determinarse el código de referencia respectivo, en esta etapa podrá ya iniciarse la reacción destinada a seguridad. De hecho, en presentaciones complejas, como es el caso de las salas de control, esta operación podrá ya discriminar los estados operativos prohibidos del sistema sometido a supervisión, y que se hayan reflejado en la visualización en pantalla. No obstante, si se identifica un código de referencia respectivo, la unidad de prueba asigna el posible valor correspondiente al parámetro de entrada, por ejemplo, en base al cuadro anteriormente mencionado. Este valor válido identificado del parámetro de entrada se verificará entonces comparándolo con el parámetro de entrada real, admitiendo, en caso necesario, una tolerancia. En el caso de que la prueba de seguridad arroje un resultado negativo, podrá iniciarse entonces la reacción relacionada con la seguridad.

[0014] Sistemáticamente, los códigos de referencia incorporan una suficiente separación y distancia de Hamming para la supresión de fallos necesaria, a fin de conseguir una diferenciación cuantificable de las diversas condiciones de visualización, así como, por consiguiente, una diferenciación cuantificable de unas condiciones de visualización desconocidas.

[0015] En principio, todos aquellos procedimientos que indiquen claramente al observador un fallo crítico para la seguridad resultarán adecuados como reacciones centradas en la seguridad. Entre las posibles reacciones centradas en la seguridad relacionadas con la aplicación pueden encontrarse, por ejemplo, la desconexión del dispositivo de presentación, bien por completo o sólo en cierta medida, permitiendo la distribución, enmascaramiento o distorsión de datos, la desconexión del ordenador, para garantizar su seguridad, o la comunicación del fallo crítico para la seguridad a una unidad jerárquicamente superior.

[0016] Por lo tanto, la unidad de comprobación realiza un examen del ordenador que es completamente independiente del mismo, utilizando unos medios especialmente sencillos y basándose en el sorprendente resultado de que todos los fallos del sistema que resultan relevantes en materia de seguridad ya han sido detectados por el examen de seguridad a través de la unidad de verificación.

[0017] Por lo tanto, el procedimiento y el dispositivo para la aplicación del procedimiento resultan completamente independientes del ordenador que genera los datos gráficos, incluyendo los componentes del sistema, como por ejemplo, el procesador, la tarjeta gráfica y similares, es decir, la tecnología informática actual, y también, especialmente, el sistema operativo. Por lo tanto, la invención se refiere a unos medios sorprendentemente sencillos y sin embargo, descubre todos los fallos relativos a la seguridad de un dispositivo informático complejo puesto bajo supervisión.

[0018] Al contrario de lo que sucede en la técnica actual, cuando se sustituyen los componentes del ordenador y se actualiza el software, ya no es necesario un certificado de seguridad acorde con el nivel de integridad de la seguridad (SIL) requerido, ya que con la introducir la prueba de seguridad realizada por la unidad de comprobación se determina la visualización de la totalidad o de parte de los datos. Por consiguiente, el procedimiento conforme a la presente invención permite en todo momento la utilización de la tecnología más avanzada con el ordenador de generación de datos gráficos sin comprometer el certificado de seguridad existente. Dicho con mayor sencillez, la

presente invención lleva a cabo una prueba especialmente sencillo de la secuencia de datos de imagen mediante su comparación con el valor del parámetro de entrada a visualizar.

[0019] De acuerdo con la comprensión por parte de los expertos del alcance de la protección de la presente invención, las señales de los parámetros de entrada, que han de transmitirse a través de unos interfaces comunes entre el ordenador, el dispositivo de presentación y la unidad de comprobación, pueden ser tanto analógicas como digitales. Los códigos de referencia pueden obtenerse mediante un circuito, como un registro de cambios, por ejemplo, o mediante programación.

[0020] Preferiblemente, la reacción destinada a seguridad será iniciada por la propia unidad de prueba, interrumpiendo la alimentación eléctrica del dispositivo de presentación, por ejemplo. No obstante, y gracias a la presente invención, también resulta posible que, a fin de iniciar la reacción destinada a seguridad, la unidad de prueba, en función del resultado de la prueba, tan sólo enviará una señal de control a otro componente del sistema o a un sistema de mayor rango jerárquico, por ejemplo, un procesador distinto de la unidad de comprobación.

[0021] Para la persona versada en la materia será evidente cómo generar unas representaciones óptimas de la imagen correspondientes a los códigos de referencia, en una etapa anterior a la operación. Por lo general, el procedimiento y el dispositivo de comprobación sugeridos para la puesta en práctica del procedimiento pueden aplicarse no solamente a representaciones de símbolos con diferentes condiciones (por ejemplo, ENCENDIDO/APAGADO), sino también a representaciones que muestren visualizaciones cuantificadas de valores de entrada analógicos, por ejemplo, instrumentos de puntero o gráficos de barras. Por ejemplo, cuando se utiliza como parámetro de entrada una tensión que oscile entre 0 voltios y 100 voltios, se puede interpretar como incrementos o reducirse a incrementos de 1 voltio cada uno, añadiendo hasta 101 representaciones unitarias en pantalla, que se muestran como un instrumento circular mediante software. De este modo, cada imagen aislada muestra la correcta posición respectiva del puntero.

[0022] Para conseguir una representación animada fiable, preferiblemente debe llevarse a cabo la prueba de seguridad mediante la realización de una prueba periódica con una frecuencia máxima equivalente al número de imágenes por segundo del dispositivo de presentación y/o de la tasa de cambio del parámetro de entrada.

[0023] En el caso de una realización especialmente preferida para identificar claramente una condición de visualización es suficiente con que una prueba de seguridad se limite a las correspondientes subáreas o segmentos de la representación de la imagen a visualizar, que caracteriza los datos específicos visualizados para el observador. Estos pueden ser las correspondientes líneas y columnas de una representación de una imagen o la punta del puntero de un instrumento circular, por ejemplo. Siempre que el área no controlada situada en el exterior de la subárea correspondiente y el área supervisada situada en el interior de la subárea correspondiente muestren diferentes contenidos, el observador podrá reconocer esta diferencia y el error no se considerará crítico para la seguridad. Por el contrario, si los datos visualizados en el área no controlada situada en el exterior de la subárea supervisada y los datos visualizados en el área supervisada situada en el interior de la correspondiente subárea fuesen diferentes entre sí, el observador podrá reconocer esta discrepancia como un error.

[0024] La práctica totalidad de los parámetros de entrada cuantificables satisfacen los requisitos anteriormente mencionados de acuerdo con la descripción. Pero mediante el procedimiento de la presente invención también se puede verificar la información textual mostrada en una sección específica del dispositivo de presentación (siempre que sea de aplicación, cada carácter alfabético único o una palabra dada presentará dicha condición de visualización).

[0025] La unidad de prueba puede consistir en un dispositivo independiente o integrado en el ordenador de generación de gráficos, así como en una unidad de supervisión independiente. Una realización controlada por software presenta la ventaja específica de que es posible incluso una mayor independencia del procesador con respecto a la plataforma y el software.

[0026] A fin de lograr una tolerancia frente a errores secuenciales, un desarrollo adicional permite que la reacción destinada a seguridad se inicie tan sólo después de un número predefinido de resultados de pruebas negativos. También puede desearse que se alcance con mayor rapidez un determinado valor de umbral necesario para desconectar el dispositivo de presentación debido a que los resultados negativos de las pruebas se tienen en cuenta con un factor más elevado, en lugar de deducir los resultados negativos por los resultados positivos.

[0027] Una posibilidad de mejorar la tolerancia a los errores horizontales consiste en considerar un resultado de una comprobación de seguridad como positivo, aun cuando el valor del parámetro de entrada corresponda a diversos valores de referencia, posibles y admisibles del parámetro de entrada resultante de la prueba de seguridad. Esto permite, en el caso de que un vehículo supervisado acelere, por ejemplo, que los códigos de referencia "adyacentes" archivados en la unidad de comprobación o adyacentes a un entorno predefinido se consideren igualmente resultados positivos de la prueba. La hora y/o el valor de las tolerancias relevantes para una aplicación respectiva podrán, por tanto, tenerse fácilmente en cuenta a la hora de generar los códigos de referencia y de llevar a cabo la prueba de seguridad.

[0028] El procedimiento y el aparato para la aplicación del procedimiento conforme a la presente invención permiten con naturalidad que varios parámetros de entrada del procesador puedan también procesarse de forma secuencial y/o paralela, comprobándose con distintos grupos de códigos de referencia en la unidad de prueba tras la generación de diversos códigos de comprobación. En principio es posible, dentro del alcance de la presente invención, facilitar diversas unidades de prueba independientes para diversas pantallas o para diversos parámetros de entrada.

[0029] Como se ha mencionado anteriormente, para la aplicación del procedimiento puede aplicarse cualquier interfaz, y por tanto, todos los medios actuales para la transmisión de datos de imagen, entre los componentes del sistema. Ichos medios pueden ser, por ejemplo, un interfaz LVDS o una señal comparable de datos digitales estandarizada para la transmisión de datos entre el procesador y el dispositivo de presentación.

Los procedimientos de codificación utilizados durante la comprobación de seguridad a fin de generar unos códigos de prueba con una determinada longitud pueden ser, por ejemplo, CRC16, CRC32 (controles de redundancia cíclica) o cualquier otro procedimiento de codificación habitual.

[0030] La comprobación de la seguridad de los diversos segmentos de las secuencias de datos de imagen puede efectuarse en la unidad de comprobación de forma paralela e independiente, a fin de garantizar un procesamiento más rápido. Los datos secuenciales de imagen pueden verse por separado, en función de sus diversos colores, por ejemplo.

[0031] En la realización preferida, la unidad de comprobación se denomina una matriz de puerta programable de campo (Field Programmable Gate Array, FPGA [disposición de puertos programable de campo]). Como es bien conocido, se trata de un circuito integrado programable utilizado en la tecnología digital, que proporciona un circuito de lógica programable conforme a la solicitud. No obstante, también puede llevarse a cabo en forma de un controlador DSP o mediante una solución de hardware, total o parcialmente.

[0032] La presente invención también hace referencia a una unidad de seguridad para la visualización de información importante para la seguridad, y especialmente para poner en práctica el procedimiento conforme a una de las reivindicaciones anteriormente mencionadas, mediante un procesador al que se le suministra al menos un parámetro de entrada a fin de transformar dicho parámetro de entrada en una secuencia de datos de imagen, y un dispositivo de presentación conectada al procesador para la visualización de la secuencia de datos de imagen. De acuerdo con el estado de la técnica actual, incluyendo las desventajas que se han descrito anteriormente, la tarea resultante de ello se realizará mediante una unidad de comprobación junto con un generador de códigos de comprobación, varios códigos de referencia conforme a la solicitud, y una unidad de referencia, calculando el generador de códigos de comprobación un código de comprobación para al menos una parte leída de la secuencia de datos de imagen. El código de comprobación resultante se compara con los códigos de referencia existentes y en caso de conformidad positiva, al código de referencia resultante se le asigna el valor correspondiente del parámetro de entrada como valor de referencia. El valor de referencia se verificará posteriormente comprobándolo con el parámetro de entrada dentro o fuera de la unidad de referencia, a fin de iniciar una reacción destinada a seguridad en caso de que la comprobación de seguridad arroje un resultado negativo.

[0033] La exactitud de la prueba de seguridad, y por tanto, de los datos sometidos a comprobación, puede verificarse desde el exterior incluyendo un valor de comprobación, por ejemplo, un numero aleatorio, en la transmisión de los datos del valor de entrada. Este valor de comprobación puede calcularse y realizarse una representación gráfica mediante el ordenador de generación de gráficos, normalmente denominado PC, o transferirse directamente al flujo de datos destinado al panel TFT, por ejemplo, como valores de índice de color de uno o más píxeles, que a continuación son directamente leídos por la unidad de comprobación o codificados de forma similar a las áreas sometidas a verificación. Junto con los códigos de las áreas sometidas a verificación, estos valores se transmiten seguidamente al ordenador de rango superior –seguro- en el que, por ejemplo, puede realizarse una comprobación temporal de los datos evaluados. Si el retardo entre la transmisión de los nuevos valores de entrada y la recepción de los valores devueltos es superior a un valor ajustable y predefinido, ello constituye una indicación evidente de que el valor real no está actualizado.

[0034] Alternativamente, el valor de comprobación/número aleatorio puede ser interpretado como un código binario por la unidad de generación de gráficos, que puede entonteces controlar diversas áreas del dispositivo de presentación, por ejemplo, haciéndolas pasar a blanco o negro, en función de un bit específico del código binario, configurado como bajo o alto.

[0035] En una realización preferida, la iluminación de estos píxeles puede verificarse situando uno o más sensores sensibles a la luz en las áreas bajo supervisión del dispositivo de presentación TFT y enviando después la señal de salida generada por dicho sensor o sensores al ordenador subordinado, como se describe en la solicitud de patente alemana DE 102004039498 A1, presentada por el solicitante. De este modo, si el número visualizado es correcto, también se devuelve el valor correcto al ordenador subordinado, lo que confirma el funcionamiento sin errores. Preferiblemente, el valor de comprobación se modifica de forma sincronizada con el cambio de los datos que van a visualizarse en el dispositivo de presentación.

[0036] En otra realización, el valor de comprobación se transmite como un patrón de bits a áreas reducidas del dispositivo de presentación, preferiblemente a áreas situadas en el borde del dispositivo de presentación, visualizándose en dichas zonas, más preferiblemente en una zona no visible o difícilmente visible para el usuario. El área visualizada vuelve entonces a leerse y se codifica como cualquier área del resto de secciones del dispositivo de presentación, o como un valor de la configuración de color de uno (o varios píxeles) (por ejemplo, el valor RGB del color), que a continuación puede ser nuevamente leído por la unidad de comprobación mediante la conexión entre el PC y el dispositivo de presentación, y que posteriormente puede ser directamente procesado o codificado por el generador de códigos. Por ejemplo, puede ser necesario que este valor de comprobación se devuelva a través de la unidad de comprobación o directamente al procesador subordinado a lo largo de un período de tiempo determinado, a fin de verificar que el sistema opera sin problemas.

[0037] Un aspecto especialmente interesante de la invención es que los valores / píxeles de comprobación anteriormente mencionados también pueden utilizarse como un contenedor de datos que, al ser transmitidos desde el ordenador, generan los datos de imagen correspondientes al valor de entrada. Como es bien conocido, cada Pixel de un dispositivo de presentación TFT está compuesto por tres píxeles subordinados de colores RGB (rojo, verde, azul). Al iluminar los píxeles subordinados, puede obtenerse cualquier color para el píxel. La invención utiliza estos píxeles como contenedores de datos para transmitir datos desde el sistema u ordenador subordinado, que genera los datos de imagen, al dispositivo de presentación. Este contenedor de datos, por ejemplo, puede ser utilizado para transmitir un valor de referencia a través de la línea existente entre el ordenador y el dispositivo de presentación. Mediante el controlador gráfico, el dispositivo de presentación puede visualizar este píxel “incorrecto” en función de su valor, pero un solo píxel es prácticamente irrelevante y apenas podrá ser percibido por un observador. También pueden evitarse las molestias para el observador utilizando los píxeles como contenedores de datos situados en las áreas exteriores del dispositivo de presentación, que pueden ser fácilmente cubiertas. No obstante, este valor de referencia puede leerse ahora directamente a través de la conexión entre el PC y el dispositivo de presentación, y transmitirse a la unidad de comprobación, por lo que no es necesario hacer que el valor de referencia describa un bucle a través del PC para transmitirlo a la unidad de comprobación. Esto presenta la ventaja crucial de que los datos de imagen generados por el ordenador y el valor de referencia correspondiente a los datos de imagen se transmiten al unísono a través del mismo canal, y ya no pueden separarse. Por ello, el valor de referencia específico siempre corresponde a los datos de imagen generados, por lo que el valor de referencia y los datos de imagen siempre están sincronizados. Por lo tanto, ya no es necesaria la previsión de tolerancias a fallos, como bucles y ciclos, durante la transmisión del valor de referencia al que se introduce en un bucle a través del ordenador, para su comparación con los datos de imagen correctos que se han leído en el dispositivo de presentación, y su posterior procesamiento por parte de la unidad de comprobación, ya que es imposible que se den diferencias entre el valor de referencia y los datos de imagen asociados. En cambio, el valor de referencia puede leerse a través de la conexión entre el ordenador y el dispositivo de presentación, normalmente una LVDS, suministrándose después directamente a la unidad de comprobación, preferiblemente en el comparador, donde se compara con el código de prueba generado por el generador de códigos.

[0038] Este píxel, que sirve como contenedor de datos, también puede utilizarse para otros aspectos que contribuyan a la mejora de la invención. Por ejemplo, puede utilizarse para almacenar y transmitir datos seguros como CRCs de datos relevantes, o como datos de cambio de área y/o rango de áreas supervisadas del dispositivo de presentación que son comprobadas por la unidad de Comprobación. Los píxeles utilizados como contenedores de datos, por ejemplo, pueden transmitir las coordenadas de la esquina superior izquierda y las coordenadas de la esquina inferior derecha de una sección supervisada del dispositivo de presentación en un caso dado. Esto significa que al cambiar las secciones supervisadas del dispositivo de presentación mediante transmitir las coordenadas de la sección supervisada con los píxeles utilizados como contenedores de datos pueden modificarse durante la operación la ubicación y/o el tamaño de las secciones supervisadas del dispositivo de presentación.

[0039] Podrán apreciarse detalles, ventajas y características adicionales de la presente invención en la siguiente descripción, que incluye una explicación detallada de una serie de ejemplos de las realizaciones preferidas del procedimiento y de los dispositivos para la aplicación del procedimiento conforme a la presente invención, haciendo referencia a las figuras, en las cuales:

La figura 1 muestra la configuración básica (diagrama esquemático) de una primera realización de un dispositivo de presentación segura conforme a la presente invención para un PC de panel, por ejemplo, en un automotor;

La figura 2 muestra un diagrama esquemático de una segunda realización de un dispositivo de presentación conforme a la presente invención;

La figura 3 muestra un diagrama esquemático de una tercera realización de un dispositivo de presentación conforme a la presente invención; y

La figura 4 muestra un diagrama esquemático de una cuarta realización de un dispositivo de presentación diseñada conforme a la presente invención.

[0040] Se ha identificado a los componentes idénticos mediante los mismos números de referencia.

[0041] La figura 1 muestra la configuración básica de una unidad de seguridad 2 para la aplicación del procedimiento en un automotor de un tren, conforme a la presente invención.

[0042] Por consiguiente, la unidad de seguridad marcada con la referencia 2 consiste básicamente en un PC 4 para generar datos de imagen representativos del procesador, y un dispositivo de presentación TFT 6 conectada a través de una LVDS 8 que comprende varios circuitos, aunque tan sólo se han mostrado esquemáticamente 3 de ellos.

[0043] La unidad de seguridad 2 también incluye una unidad de comprobación diseñada como una comprobación de un interfaz FPGA 10 y de unidades de microcontroladores, denominada simplemente FPGA 10.

[0044] En el ejemplo que se muestra, un parámetro de entrada en forma de un valor de velocidad (V_{actual}) indicado con la referencia 14 y que puede originarse, por ejemplo, en un ordenador principal, de acuerdo con las normas y reglamentos ordinarios en materia de seguridad, u “ordenador seguro”, se comunica a un PC 4. Este valor puede transmitirse en bucle a través del PC 4 y transmitirse a la unidad de comprobación segura 10 a través de un circuito de entrada 26. Alternativamente, el valor del parámetro de entrada 14 también puede transmitirse directamente al FPGA 10.

[0045] El PC 4 transmite la información relevante para la seguridad a través de la línea del dispositivo de presentación 36 para su visualización en un área supervisada delimitada 16 del dispositivo de presentación TFT 6. La información relevante para la seguridad se muestra en forma de un mapa de bits “pre-renderizado” y, por consiguiente, predefinido de una forma definida en el dispositivo de presentación TFT 6.

[0046] La señal de entrada de alta frecuencia del dispositivo de presentación TFT 6 suministrada a través de una línea de la LVDS 8 es leída por la FUGA 10 en uno u otro sentido a través de la línea de relectura 22.

[0047] Para llevar a cabo la prueba de seguridad, la unidad de comprobación de seguridad 10 genera una suma de control CRC en un generador de códigos de comprobación 12 para el mapa de bit pre-renderizado del área supervisada 16, generando de este modo una "huella dactilar" de esta área supervisada 16 en un momento dado. Cada mapa de bit generado por el PC 4 tiene asignado claramente un valor checksum CRC previamente calculado como código de referencia de acuerdo con un cuadro 18 de la FPGA 10 y se facilita un posible valor del parámetro de entrada 14 para cada uno de estos códigos de referencia.

[0048] En primer lugar, la unidad de comprobación segura 10 compara el código de comprobación calculado por el generador de códigos de referencia 12 con los códigos de referencia según el cuadro 18. Si el código de comprobación se ajusta a un código de referencia indicado en el cuadro 18, el posible valor del parámetro de entrada, de acuerdo con el cuadro 18, se compara mediante un comparador 20 con el valor del parámetro de entrada almacenado en una memoria 24. Si se determinan discrepancias inadmisibles durante el proceso, podrá iniciarse una reacción ante fallos de seguridad mediante la interrupción del circuito de la fuente de alimentación 28 del dispositivo de presentación TFT 6 mediante la línea de interrupción 34.

[0049] Un factor decisivo para la evaluación de seguridad de la visualización de la velocidad es la visualización puntual del correspondiente valor de velocidad dentro de unas tolerancias de tiempo y valor, admisibles.

[0050] La función de desconexión activada por el interfaz FPGA 10 en esta realización funciona de acuerdo con el principio de “corriente de circuito cerrado” (equivalente a circuitos de relés relacionados con la seguridad) de forma que, para que se inicie la unidad de comprobación se necesita una activación para mantener el estado de funcionamiento normal, mientras que, en el caso de que la unidad de comprobación no funcione o esté desconectada ("pasivación") se inicia una reacción de fallo de seguridad.

[0051] La realización alternativa de un dispositivo de presentación de acuerdo con la presente invención y que se muestra en la figura 2 sirve para transmitir el resultado negativo de la comprobación resultante de la comprobación de seguridad en la unidad de comprobación segura 10 a través de un circuito de realimentación 30 a un procesador de rango jerárquico superior 32 que iniciará entonces la reacción destinada a seguridad, como por ejemplo, desacelerar el automotor. Alternativamente, esta transmisión también puede efectuarse de forma inalámbrica, lo que por supuesto es de aplicación a todos los tipos de señal. Este procesador subordinado 32, por ejemplo, puede formar parte del mismo ordenador “seguro”, generando el valor real 14 que se comunica al PC 4.

[0052] La realización simplificada que se muestra en la figura 3 difiere de las que se muestran en las figuras. 1 y 2 en que la unidad de comprobación segura 10 comprende básicamente tan sólo el generador de códigos de comprobación 12 para la generación del código para la “huella dactilar” o área delimitada 16 del dispositivo de presentación 6. En esta realización, las etapas adicionales de la prueba de seguridad se pueden realizar en el exterior de la unidad de comprobación segura 10, por ejemplo en el procesador subordinado 32, también denominado “ordenador seguro”, lo que simplifica aún más el diseño de la unidad de comprobación 10.

[0053] En la realización que se muestra en la figura 4, el parámetro de entrada 14 no recorre un bucle a través del PC 4. En cambio, el parámetro de entrada 14, junto con la imagen correspondiente al parámetro de entrada 14 generada por el PC 4 se transmite a través de la línea del dispositivo de presentación 36 de la LVDS 8 y se leen

ambos a través de la línea 38 conectada al generador de códigos 12, a fin de evitar una posible falta de sincronización entre el parámetro de entrada 14 y los datos de imagen generados por el PC 4, devolviéndose después a la unidad de comprobación 10 a través de la línea relectura 22, lo cual puede suceder en caso en el caso de que la transmisión del parámetro de entrada 14 no está sincronizada correctamente en la realización conforme a la figura 1.

Lista de referencias

2	Unidad de seguridad
4	PC (Ordenador de generación de datos de imagen)
6	Pantalla TFT
8	LVDS
10	Unidad de comprobación segura (FPGA)
12	Generador de códigos de comprobación
14	Valor de velocidad
16	Área supervisada
18	Cuadro
20	Unidad de referencia
22	Línea relectura
24	Memoria
26	Circuito de entrada
28	Circuito de alimentación
30	Circuito de feed back
32	Procesador de rango jerárquico superior
34	Línea de interrupción
36	Línea de visualización

REIVINDICACIONES

1. Procedimiento para la representación segura de información relativa a seguridad que comprende: introducir, al menos, un parámetro de entrada en un procesador, procesar por ordenador el parámetro de entrada, transformándolo en una secuencia de datos de imagen que representan el parámetro de entrada, transmitir la secuencia de datos de imagen a un dispositivo de presentación (6) para representar la secuencia de datos de imagen en dicho dispositivo de presentación (6), caracterizado porque la secuencia de datos de imagen se transmite a una unidad de prueba (10), efectuándose una comprobación de seguridad mediante generación por ordenador de un código de comprobación correspondiente a la secuencia de datos de la imagen, verificándose dicho código de comprobación con diversos códigos de referencia, asignándose el código de referencia identificado en ese momento con el correspondiente valor posible del parámetro de entrada y comprobándose con el valor del parámetro de entrada mediante la unidad de comprobación, la cual genera un resultado de la comprobación positivo o negativo para provocar una reacción destinada a seguridad.

2. Procedimiento conforme a la reivindicación 1, caracterizado porque los códigos de referencia se encuentran integrados en la unidad de comprobación (10).

3. Procedimiento conforme a la reivindicación 1 o 2, caracterizado porque la reacción destinada a seguridad se inicia en la unidad de comprobación cuando la comprobación de seguridad desemboque en un resultado negativo,

o

en un procesador diferente de la unidad de comprobación (10) si la comprobación de seguridad arroja un resultado negativo.

4. Procedimiento conforme a una de las reivindicaciones 1 a 3, caracterizado porque la reacción destinada a seguridad incluye el dispositivo de presentación a desconectar.

5. Procedimiento conforme a una de las reivindicaciones 1 a 4, caracterizado porque la reacción destinada a seguridad, sólo se inicia después de un número predeterminado de resultados negativos o porque una comprobación de seguridad se considera un resultado positivo de la prueba, aun cuando el valor del parámetro de entrada corresponda a varios de los posibles valores de referencia admisibles del parámetro de entrada.

6. Procedimiento conforme a una de las reivindicaciones precedentes, caracterizado porque se procesan varios parámetros de entrada en el procesador, porque las correspondientes secuencias de datos de imágenes se transmiten a una o varias pantallas (6) y se visualizan en las mismas, generándose y comprobándose el correspondiente código de comprobación para las secuencias de datos de imágenes.

7. Procedimiento conforme a la reivindicación 6, caracterizado porque los diferentes parámetros de entrada de las diversas secuencias de datos de imagen se representan en zonas limitadas (16) del dispositivo de presentación (6).

8. Procedimiento conforme a una de las reivindicaciones 5 a 7, caracterizado porque las diferentes secuencias de datos de imagen se comprueban en la unidad de comprobación (10) de forma paralela e independiente.

9. Procedimiento conforme a una de las reivindicaciones precedentes, caracterizado porque la sección a supervisar se limita a un segmento que caracteriza por completo el parámetro de entrada a visualizar por el observador.

10. Procedimiento conforme a una de las reivindicaciones de procedimiento precedentes, caracterizado porque al parámetro de entrada se añade un valor de comprobación y se evalúa el valor devuelto para dicho valor de comprobación.

11. Procedimiento conforme a la reivindicación 10, caracterizado porque el valor de comprobación se incluye en un píxel que sirve de contenedor de datos.

12. Procedimiento conforme a una de las reivindicaciones 10 u 11, caracterizado porque el píxel que sirve de contenedor de datos se utiliza para influir sobre el procesamiento por ordenador.

13. Procedimiento conforme a la reivindicación 12, caracterizado porque el píxel se utiliza para modificar el área y/o el rango de las áreas supervisadas (16) del dispositivo de presentación.

14. Procedimiento conforme a una de las reivindicaciones de procedimiento precedentes, caracterizado porque el parámetro de entrada se transmite a la unidad de comprobación (10) en un flujo de datos desde el procesador que genera los gráficos paral dispositivo de presentación (6).

15. Procedimiento conforme a una de las reivindicaciones de procedimiento precedentes, caracterizado porque conjuntamente con el parámetro de entrada, los códigos de referencia específicos se entregan a la unidad de comprobación (10) para su comparación con el código generado a partir de la visualización actual.

16. Unidad de seguridad, especialmente para aplicar el procedimiento conforme a una de las reivindicaciones anteriormente mencionadas, equipada con un procesador al que se suministra, al menos, un parámetro de entrada, para transformación de éste último en una secuencia de datos de imagen, y con un dispositivo de presentación (6) conectada al procesador, para representación de los datos de imagen, caracterizada por una unidad de comprobación (10) que incluye un generador de códigos de comprobación (12), diversos códigos de referencia específicos de la aplicación y una unidad de referencia (20) , donde el generador de códigos de comprobación (12) genera un código de comprobación para, al menos, una parte leída de la secuencia de datos de imagen, comparando el código de comprobación generado de este modo con los códigos de referencia existentes y, en caso de ser conformes entre sí, asignar al código de referencia identificado de esta forma, el correspondiente valor del parámetro de entrada como valor de referencia, comparando después este valor de referencia con el parámetro de entrada en la unidad de referencia (20) a fin de iniciar una reacción destinada a seguridad en caso de no conformidad, es decir, en caso de que la comprobación arroje un resultado negativo.

Fig. 1

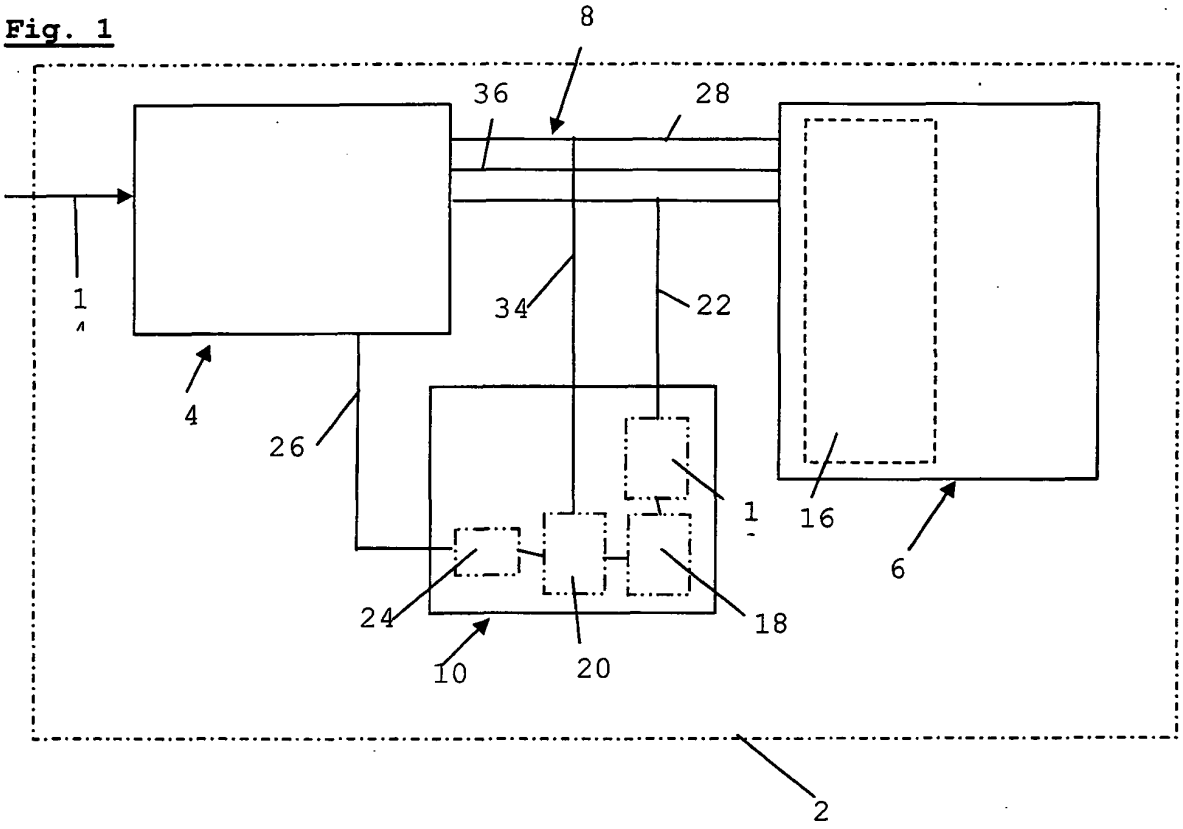


Fig. 2

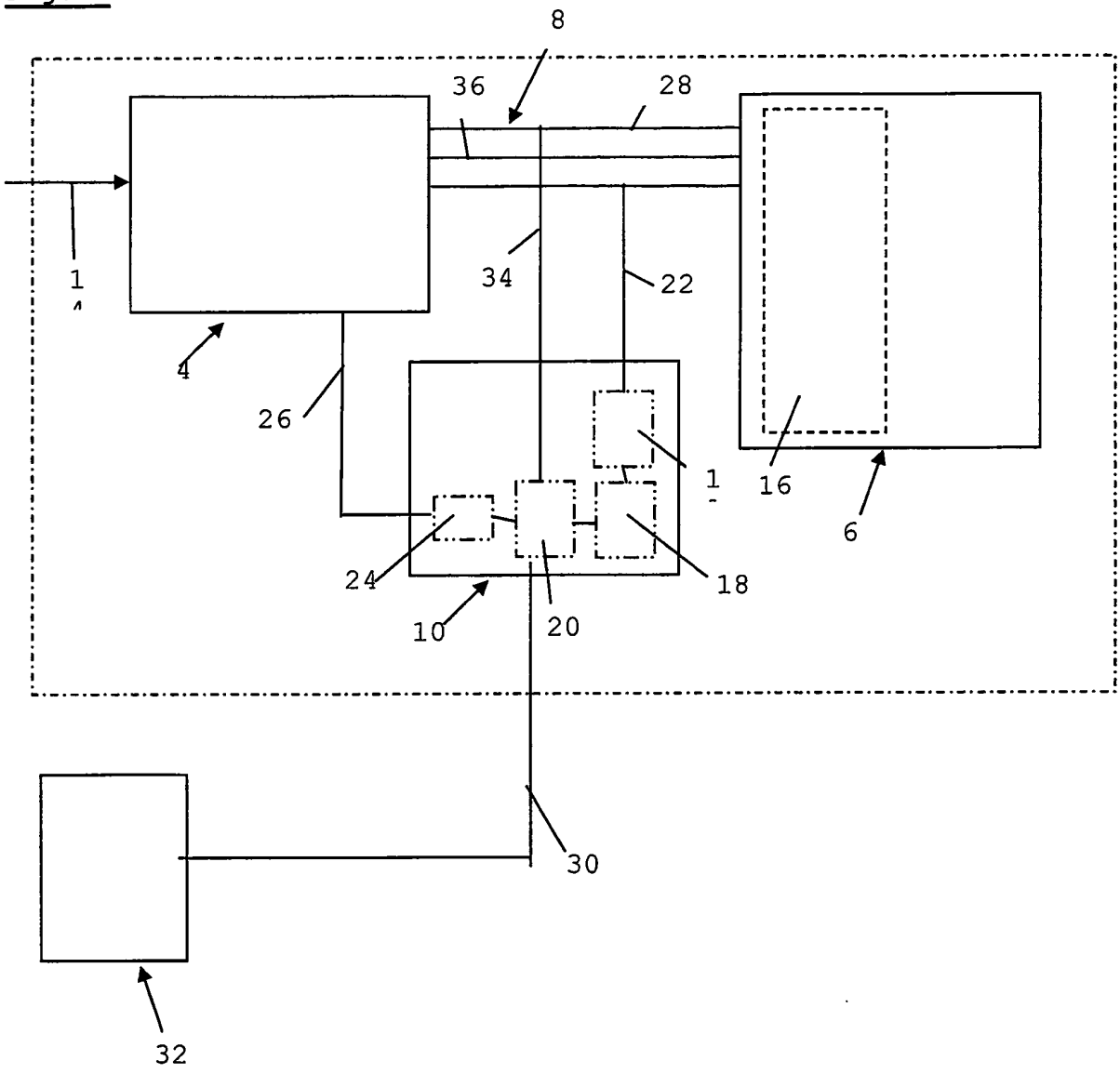


Fig. 3

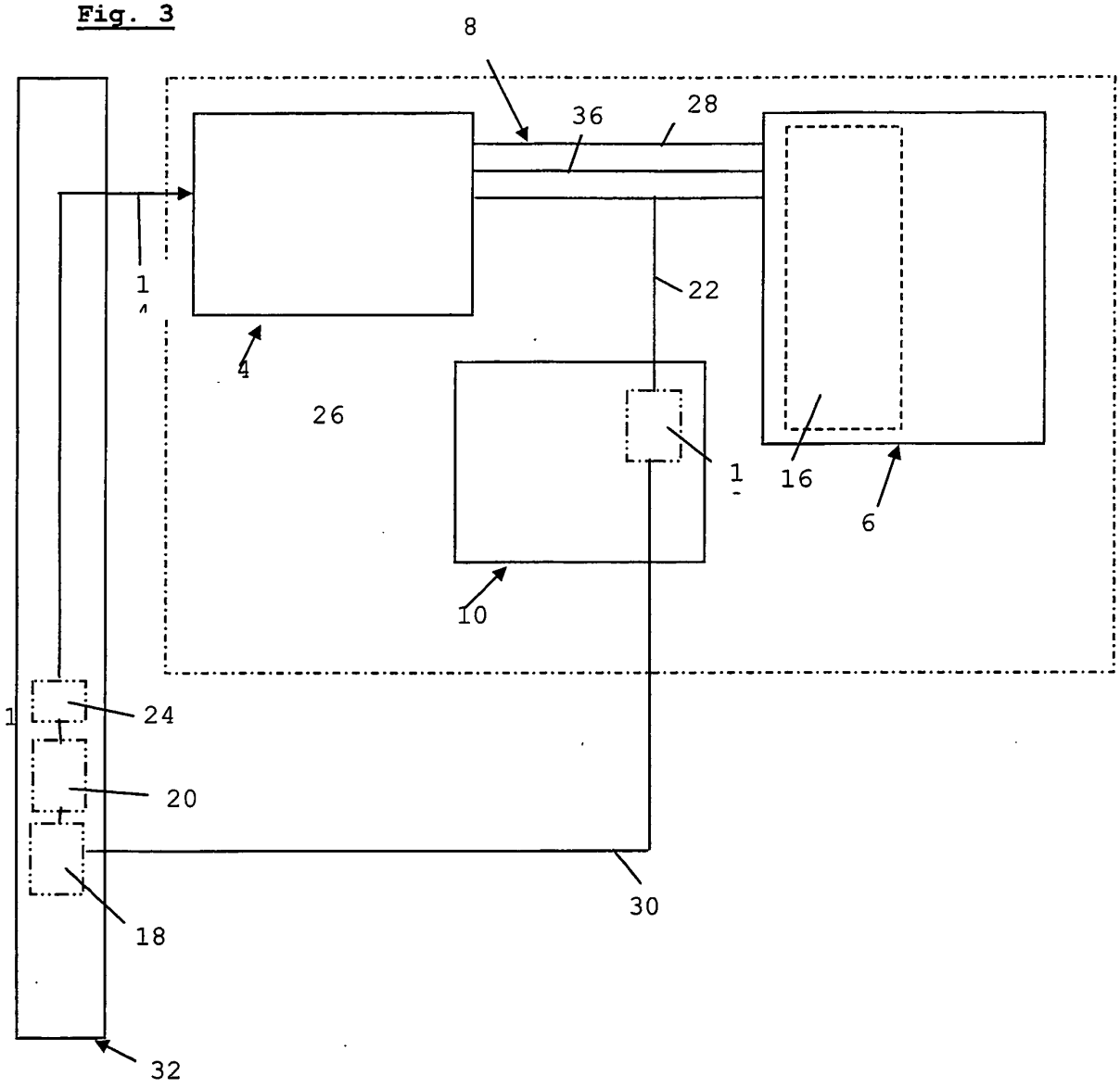
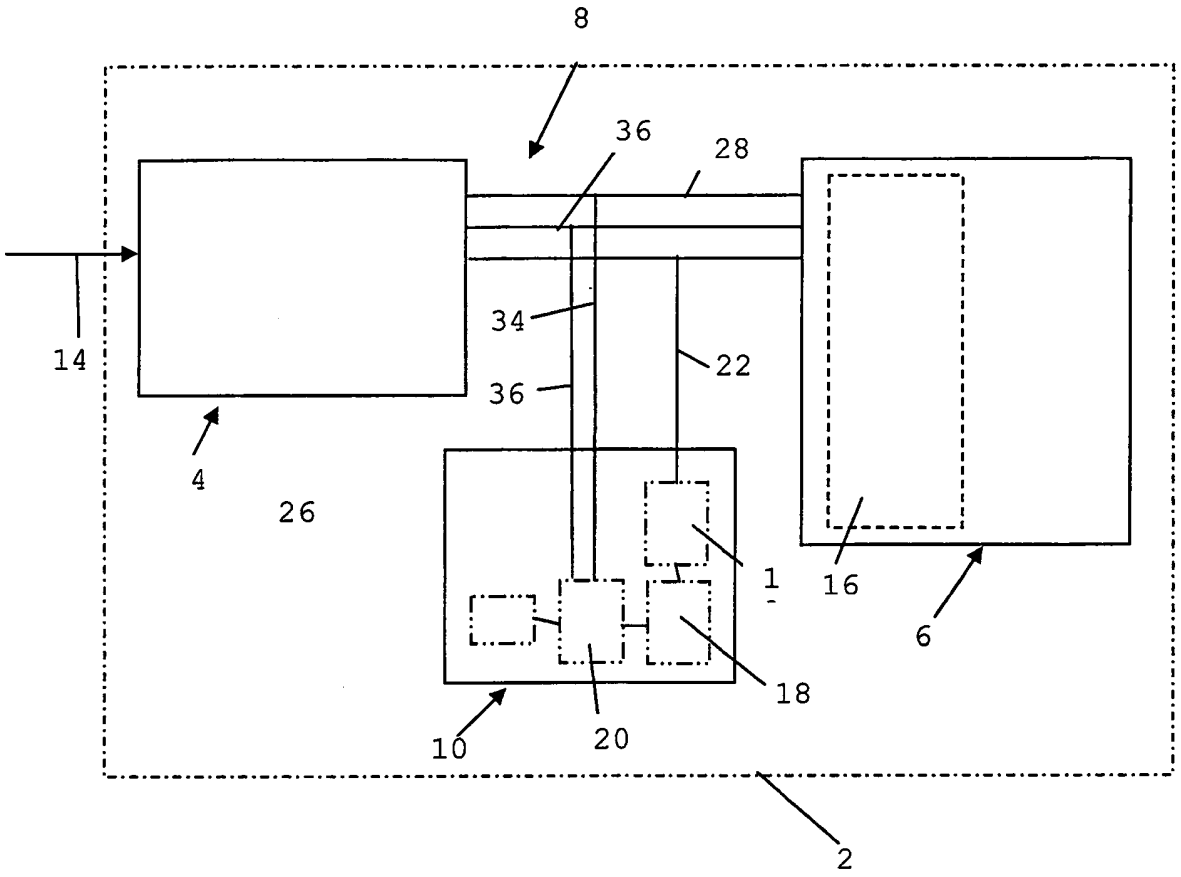


Fig. 4



REFERENCIAS CITADAS EN LA DESCRIPCIÓN

La lista de referencias citada por el solicitante lo es solamente para utilidad del lector, no formando parte de los documentos de patente europeos. Aún cuando las referencias han sido cuidadosamente recopiladas, no pueden excluirse errores u omisiones y la OEP rechaza toda responsabilidad a este respecto.

Documentos de patente citados en la descripción

- DE 4332143 A **[0008]**
- EP 0856792 A **[0008]**
- DE 102004039498 A1 **[0035]**