(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 436 609**

(51) Int. CI.:

G06F 11/18 (2006.01)
H04L 12/403 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.05.2006 E 06114053 (9)**

(97) Fecha y número de publicación de la concesión europea: **23.10.2013 EP 1857935**

(54) Título: **Nodo de bus de datos de tolerancia de fallos en un sistema distribuido**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.01.2014

(73) Titular/es:

SAAB AB (100.0%)
581 88 Linköping, SE

(72) Inventor/es:

JOHANSSON, RIKARD y
WISTEDT, KJELL

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Nodo de bus de datos de tolerancia de fallos en un sistema distribuido

Campo técnico de la invención

La invención se refiere, en general, al campo de los sistemas de tolerancia de fallos y, más en concreto, a la materia objeto de la porción precaracterizadora de la reivindicación independiente 1.

Antecedentes

Los sistemas de (control) de datos de tolerancia de fallos son utilizados, por ejemplo, en aplicaciones aeronáuticas que requieren una integridad muy elevada. Los sistemas convencionales de control aeronáutico de tolerancia de fallos se basan en una comunicación punto a punto entre computadora/s sensor/es y accionador/es.

El problema asociado con los sistemas convencionales aeronáuticos de tolerancia de fallos se refiere al peso, la complejidad, a la disponibilidad del procesamiento de datos y al coste.

El artículo “GESTIÓN DE REDUNDANCIA EN SISTEMAS DE CONTROL DE VUELO DISTRIBUIDOS: EXPERIENCIA Y SIMULACIONES” [“REDUNDANCY MANAGEMENT IN DISTRIBUTED FLIGHT CONTROL SYSTEMS: EXPERIENCE AND SIMULATIONS”], de K. Ahlström et al., publicado por el IEEE 2002, describe un sistema de control en tiempo real de tolerancia de fallos para aplicaciones aeronáuticas que comprende unos nodos de control diseñados con un alto grado de detección de fallos embebido. Una simulación del sistema se basa en la presunción de que todos los nodos envían datos (sobre el bus) estrictamente en sus intervalos de tiempo debido al hecho de que una guarda de bus de cada nodo de bus de los fallos de “palabrería sin sentido” [babbling idiot]. Un inconveniente de este diseño es que los nodos que funcionan de hecho correctamente pueden quedar bloqueados en la transmisión sobre el bus debido a un mal funcionamiento de la guarda de bus.

El artículo “Una Guarda de Bus Analizable para la Comunicación de Episodios Desencadenados” [An Analyzable Bus - Guardian for Event - Triggered Communications”] de I. Brooster & Burns publicado por el Vigesimo Cuarto Simposium del Sistemas en Tiempo Real Internacional del IEEE [“24: th IEEE International Real - Time Systems Symposium”] describe diversas estrategias / arquitecturas de guarda de bus. Una de dichas estrategias / arquitecturas presenta una guarda como un nodo completamente separado conectado directamente a un bus (TDMA). Utilizando solo la información procedente del bus, el nodo de guarda vigila las transmisiones sobre el bus y detecta los nodos de palabrería. El nodo guarda está dispuesto para afectar (cerrar) un nodo de palabrería utilizando un nodo directo sobre el nodo de palabrería. Un problema de este tipo de estrategia / arquitectura es que el guarda es solo capaz de detectar un nodo de palabrería después de que ha sido transmitido un mensaje incorrecto sobre el bus.

Un problema general de los sistemas de datos de bus de TDMA de tolerancia de fallos es el problema de la “palabrería sin sentido”, esto es, que un nodo transmite sobre el bus en un intervalo de tiempo que no está dedicado a ese nodo.

El artículo “Evitación del Fallo de la Palabrería sin Sentido en un Sistema de Comunicación Desencadenado en el Tiempo” [“Avoiding the babbling - idiot failure in a time - triggerd communication systems”] de C. Temple, publicado por el IEEE, COMPUTACIÓN DE TOLERANCIA DE FALLOS, 1998. COMPENDIO DE DOCUMENTOS. VIGÉSIMO OCTAVO SIMPOSIO INTERNACIONAL ANUAL 23 - 25 JUNIO 1998 [FAULT - TOLERANT COMPUTING, 1998. VIGEST OF PAPERS. TWENTY - EIGHTH ANNUAL INTERNATIONAL SYMPOSIUM 23 - 25 JUNE 1998] describe un sistema de datos de bus de TDMA, en el que cada nodo de bus comprende una guarda de bus que acciona el conmutador de aislamiento del bus de nodos.

Sumario de la invención

Constituye un objetivo de la presente invención proporcionar unos procedimientos y unos medios que resuelvan / mitiguen los problemas analizados con anterioridad.

Constituye un objetivo de la presente invención proporcionar un sistema de datos de tolerancia de fallos que comprenda un conjunto de nodos de control de procesamiento de datos que está dispuesto para comunicar a través de un bus de TDMA en el que una pluralidad de nodos de dichos nodos comprende cada uno un mecanismo de guarda bus para suprimir un comportamiento de transmisión defectuoso del nodo respectivo, sistema de datos que resuelve de manera eficaz el problema de la palabrería sin sentido analizada con anterioridad y sistema que muestra un comportamiento potenciado global de silenciamiento de los datos sin comprometer las características del peso / disponibilidad del sistema.

De acuerdo con un primer aspecto, la invención proporciona un nodo de bus de datos, que es un nodo de control o un nodo sensor y que está dispuesto para comunicar a través de un bus de datos de TDMA, comprendiendo el nodo:

- un dispositivo de procesamiento de señal de tiempo que está configurado para definir un programa de transmisión de intervalos de tiempo de TDMA para al menos dicho nodo,

- un conmutador que está configurado para conectar una vía de transmisión de dicho nodo con el bus o bien aislarla y que está configurado para ser controlado por dicho programa de transmisión de intervalo de tiempo de TDMA de dicho nodo por medio de un dispositivo de control de acceso de transmisión de bus, estando dicho nodo caracterizado porque,

- dicho dispositivo de control de acceso de transmisión por bus está configurado para ser también controlado por al menos una señal de control externa por medio de al menos un enlace de transmisión de datos externo que está físicamente separado de dicho bus.

La invención elimina de esta manera la necesidad de dobles relojes, esto es, dobles programas de TDMA, en el nodo, para obtener una supresión de la transmisión defectuosa. En su lugar, el nodo puede explotar, por ejemplo, los programas de TDMA preprogramados y / o las señales de control de otros nodos por medio del enlace de comunicación externo con el fin de suprimir su comportamiento de transmisión defectuoso, esto es, suprimir un comportamiento de palabrería sin sentido y / o soportar un comportamiento de fallo silente. Dado que el enlace de comunicación está físicamente separado del bus, un comportamiento de palabrería sin sentido puede ser bloqueado inmediatamente para que las transmisiones “defectuosas” sean bloqueadas y no sean nunca transmitidas sobre el bus. Así mismo, la viabilidad de datos global y el ancho de banda eficaz del bus no están comprometidos en modo alguno.

El nodo puede comprender un dispositivo lógico que está configurado para:

- recibir y procesar al menos dos señales de control de entrada procedentes de una pluralidad de nodos asociados con el bus por medio de dicho/s enlace/s de transmisión de datos externo/s, y

- emitir una señal de control, que es una función de dichas recibidas al menos dos señales de control de entrada, sobre el dispositivo de control de acceso de transmisión por bus.

Permitir decisiones “de parlamento electrónico” eficaces, esto es, una decisión inteligente basada en una diversidad, para el dispositivo de control de acceso de transmisión por bus.

El dispositivo de control de acceso de transmisión por bus puede ser llevado a la práctica como un comparador y dicho dispositivo lógico puede ser llevado a la práctica como un comparador.

Proporciona una realización simple, rentable.

El nodo puede también comprender un dispositivo de vigilancia del circuito de guarda para establecer si el propio nodo está funcionando correctamente o no y dicho dispositivo de control de acceso de transmisión por bus puede también ser controlado por el dispositivo de vigilancia del circuito de guarda.

[Permite un comportamiento potenciado adicional de fallo silente del nodo dado que cualquier energización incorrecta del nodo según se identifica por el dispositivo de suministro correcto de energía puede bloquear también las transmisiones sobre el bus].

El programa de transmisión de intervalo de tiempo de TDMA puede también definir unos intervalos de transmisión para al menos otro nodo asociado con el bus, y el propio nodo puede estar dispuesto para:

- formar una señal de control de salida que sea una función de dicho programa de transmisión de intervalo de tiempo de TDMA, y

- emitir dicha señal de control sobre al menos otro nodo a través de un enlace de transmisión de datos externo que está físicamente separado de dicho bus.

[Permite la creación de grupos de nodos eficaces en el que cada nodo comprende un dispositivo de procesamiento de señal de tiempo configurado para definir un programa de transmisión de intervalo de tiempo de TDMA para todos los nodos del grupo y en el que los nodos del grupo explotan el programa de TDMA de cada uno de los demás para una supresión de transmisión defectuosa eficaz. Más en concreto, el comportamiento de la palabrería sin sentido de un nodo asociado con el bus puede eficazmente ser suprimido de esta manera]

El nodo puede también comprender un dispositivo de vigilancia para vigilar las señales de control emitidas a través del bus por otros nodos de control u otros datos de detección transmitidos a través del bus por los nodos de detección asociados con el bus, y el dispositivo de vigilancia puede estar dispuesto para:

- establecer un estado de funcionamiento incorrecto de un nodo de funcionamiento incorrecto asociado con el bus, en base a dicha vigilancia y,

- emitir una señal de control de bloqueo de transmisión para bloquear otras transmisiones del nodo de funcionamiento incorrecto en respuesta al estado de funcionamiento incorrecto así establecido del nodo de funcionamiento incorrecto,

y en el que el propio nodo puede estar configurado para formar dicha/s señal/es de control de salida como una función de dicha señal de control del bloqueo de transmisión.

[Esto proporciona un control eficaz internodos que potencia el comportamiento de fallo silente del / de los nodo/s. Así mismo, dado que el dispositivo de vigilancia ventajosamente está siendo realizado por medio de software, la invención proporciona una solución que hace fácil actualizar / configurar / adaptar un sistema de datos de bus, por ejemplo en una etapa tardía del curso del trabajo del diseño del sistema, sin comprometer la integridad / complejidad / peso global del sistema].

El nodo puede contener un dispositivo de vigilancia del circuito de guarda para establecer si el propio nodo está funcionando incorrectamente o no en el que el nodo está configurado para formar dicha señal de control de salida como una función de la señal de control de salida de vigilancia del circuito de guarda emitida por el dispositivo de vigilancia del circuito de guarda indicativa de si el nodo está funcionando incorrectamente o no.

[Eficazmente bloquea esta influencia de los nodos sobre otras transmisiones de bus de nodos sobre el bus en caso de que este nodo propiamente dicho esté funcionando incorrectamente].

El nodo puede también comprender un dispositivo de suministro correcto de energía para establecer si el propio nodo está siendo energizado de una forma correcta y en el que el nodo está configurado para formar dicha señal de control de salida como una función de una señal de control de dicho dispositivo de suministro correcto de energía.

[Eficazmente bloquea esta influencia de los nodos sobre las transmisiones de bus de otros nodos sobre el bus en el caso de que el suministro de energía de este nodo mismo esté funcionando incorrectamente].

De acuerdo con un segundo aspecto, la invención proporciona un sistema de bus de tolerancia de fallos que comprende al menos dos nodos de bus, que son nodos de control - de detección que están dispuestos para comunicar a través del bus de TDMA, en el que una pluralidad de dichos nodos comprenden cada uno un mecanismo de guarda del bus para suprimir un comportamiento de transmisión defectuoso en el que un sistema comprende un nodo de acuerdo con un primer aspecto de la invención.

[Proporciona un sistema de bus de datos de tolerancia de fallos el cual de una manera sencilla puede ser actualizado en un sistema de bus de datos seguros (palabrería sin sentido) / (fallo silente) con incremento de la integridad. Todo lo que se requiere es instalar un segundo nodo de acuerdo con cualquiera de las reivindicaciones 1 a 9 y conectarlo, por medio de un enlace de transmisión de datos que esté físicamente separado del bus, con el primer nodo existente de acuerdo con cualquiera de las reivindicaciones 1 a 9].

El sistema de bus de datos de tolerancia de fallos puede estar configurado para que al menos dos de dichos nodos estén conectados por medio de al menos un enlace de transmisión de datos que esté típicamente separado de dicho bus, permitiendo con ello al menos un mecanismo de guarda de bus de uno de los nodos así conectados para emitir una señal de control hacia el mecanismo guarda de bus de otro de los nodos así conectados a través de dicho enlace de transmisión.

[Dado que los mecanismos de guarda de bus de los nodos individuales de acuerdo con la invención pueden comunicar de esta manera, y por tanto controlarse / bloquearse entre sí, a través del enlace de comunicación que está físicamente separado del bus, pueden también potenciar su respectivo comportamiento de fallo silente por medio de la supresión de transmisiones defectuosas mutuas. Más en concreto, la invención permite de esta manera el bloqueo inmediato de las transmisiones “palabrería” defectuosas, esto es, “transmisiones desde un nodo de control (de funcionamiento incorrecto) hacia fuera de su intervalo de tiempo dedicado y para que sean eficazmente bloqueadas y no sean transmitidas desde el bus. Así mismo, de esta manera cada nodo puede obtener una diversidad de supresiones de transmisiones defectuosas mediante la explotación del / de los reloj/es del / de los programa/s, de transmisión de otros nodos, esto es, solo se necesita implantar un reloj y un programa de transmisión de bus en cada nodo, lo que directamente se traduce en una reducción del peso del sistema. Así mismo, dado que la invención elimina la necesidad de un nudo de guarda de bus puro para vigilar / bloquear los nodos de control, la invención proporciona una seguridad de sistema incrementada y una complejidad / coste peso del sistema reducidas, al mismo tiempo].

El sistema de bus de datos de tolerancia de fallos puede estar configurado para que al menos tres de dichos nodos estén mutuamente interconectados entre sí por medio de enlaces de transmisión que estén físicamente separados de dicho bus, creando de esta manera un grupo de al menos tres nodos que controlan mutuamente el mecanismo de guarda del bus de los demás nodos por medio de dichos enlaces de transmisión de datos.

[Proporciona la posibilidad de obtener unas decisiones de transmisión de bus eficaces con una diversidad de decisiones de al menos 3 unidades independientes. Esto significa que se reduce drásticamente la posibilidad de que un nodo de funcionamiento incorrecto influencie / controle de hecho un nodo de funcionamiento correcto, lo que directamente se traduce en un incremento de la integridad del sistema].

El sistema de bus de datos de tolerancia de fallos puede comprender un nodo que esté conectado con un sensor por medio de una interfaz análoga que esté separada del bus de datos y en el que el nodo de control esté dispuesto para leer valores de muestra procedentes del sensor a través de dicha interfaz análoga.

[Esta solución puede ser ventajosa en entornos / aplicaciones en las que un nodo de detección está alejado de, y no necesariamente necesita comunicar, con el bus, otros nodos de control pueden necesitar comunicar con al menos un nodo de control. De esta manera, el nodo de detección en cuanto tal, no necesita la protección de la palabrería sin sentido, lo que reduce la complejidad / coste].

El sistema de bus de datos de tolerancia de fallos puede realizarse para que se realice dicho/s enlace/s de transmisión de datos externo/s que esté físicamente separado del bus como:

- un circuito eléctrico, por ejemplo en forma de cable, hilo, fibras ópticas o línea de entrada compuesta por un material eléctricamente conductor,
- un enlace de radiocomunicación, por ejemplo un enlace inalámbrico Bluetooth™,
- un enlace de comunicación de infrarrojo,
- un enlace de transmisión de datos por sonar,

o combinaciones de estos.

[Permite una satisfactoria funcionalidad de los nodos en una amplia gama de entornos / aplicaciones, como por ejemplo en aplicaciones bajo el agua, etc.].

De acuerdo con un tercer aspecto, la invención proporciona una aeronave que comprende un nodo de bus de datos de acuerdo con el primer aspecto de la invención, o un sistema de datos de tolerancia de fallos de acuerdo con el segundo aspecto de la invención.

[Proporciona una aeronave que incorpora un sistema de datos con una integridad incrementada y un peso reducido].

Aun cuando la invención ha sido resumida en las líneas anteriores, la invención se define por las reivindicaciones 1 a 15 que se acompañan.

Breve descripción de los dibujos

Las características distintivas y las ventajas de la presente invención se pondrán de manifiesto de una forma más acabada a partir de la descripción detallada subsecuente de las formas de realización preferentes con referencia a los dibujos que se acompañan, en los que:

La FIG. 1 muestra un ejemplo ilustrativo de un sistema 100 de datos de tolerancia de fallos de acuerdo con una forma de realización de la invención,

la FIG. 2 ilustra la forma en que un comportamiento de la palabrería sin sentido de un nodo es eficazmente suprimido de acuerdo con la invención.

Descripción detallada de formas de realización preferentes

A continuación, con referencia a las FIGS. 1 – 2,.se describirá con mayor detalle la presente invención.

La invención se describirá aquí con detalle para la forma de realización específica en la que el sistema de datos de tolerancia de fallos se lleva a cabo como un sistema de control de vuelo distribuido, pero es evidente para la persona experta en la materia que el sistema de datos de tolerancia de fallos de acuerdo con la invención puede ser utilizado para otras muchas aplicaciones que exploten los nodos de procesamiento de datos que comunican a través de un bus de datos de TDMA.

Terminología:

Nodo de control: un nodo de procesamiento de datos conectado a un bus de datos y que procesa los datos de información de control relevantes para emitir señales de control hacia accionadores (nodos accionadores) sobre el bus.

Nodo de control de fallo silente: un nodo de control que muestra solo un único modo de fallo, de *fallo silente*, es designado como un nodo de control de fallo silente. En general, un nodo de control es considerado de fallo silente si produce o bien resultados correctos o ningún resultado en absoluto. El comportamiento de fallo silente asegura que un error dentro de un nodo de control no se propague a otros nodos de control dentro del sistema de forma que el nodo pueda ser considerado como una región de contención de fallos separada.

Nodo accionador: un nodo que comprende un accionador para regular un dispositivo, por ejemplo, para regular una superficie de control de un ala de un aeroplano, y que está dispuesto para regular dicho dispositivo de acuerdo con la señal de control recibidas procedente de los nodos de control.

Nodos de detección: un nodo que comprende algún dispositivo de medición para establecer un valor de integridad física, como por ejemplo la posición angular de una superficie de control de un ala en un aeroplano, y dispuesto para comunicar el valor de entidad física establecida hacia al menos un nodo de control a través del bus.

Servonodo: un nodo accionador que está integrado con un nodo de detección. Así, un servonodo debe ser interpretado como es también un nodo de detección de acuerdo con la invención.

Nodos de guarda de bus: nodos dispuestos para simplemente vigilar, y posiblemente bloquear la transmisión de los nodos de control (de funcionamiento incorrecto), se designan como nodos de guarda de bus. Así , estos nodos no transmiten ninguna señal de control sobre el bus hacia los nodos accionadores.

La FIG. 1 ilustra de manera esquemática un ejemplo ilustrativo de un sistema 100 de bus de datos de tolerancia de fallos de acuerdo con la invención, bajo la forma de un sistema de control de vuelo distribuido e instalado en un aeroplano (no ilustrado). El sistema 100 comprende un conjunto de nodos 110, 120, 130 de control de fallo silente, conectado a un bus 105 de TDMA. Unos servonodos 140, 150 están también conectados al bus 105. Los servonodos 140, 150 en este ejemplo ilustrativo pueden, por ejemplo, regular una respectiva superficie de control de un ala respectiva del aeroplano.

El nodo 110 de control, aquí designado como nodo A, comprende un bloque 1100 software el cual por razones de claridad ha sido dividido en un dispositivo 1110 de programación de transmisión de TDMA, un dispositivo 1120 convencional de servocontrol de comparación y una computación convencional del dispositivo 1130 de servocomando. El bloque software se pone en práctica normalmente por medio de un software bajo la forma de un medio de código de programa que es ejecutado por un dispositivo de procesamiento de datos, por ejemplo una microcomputadora o una UCP (no ilustrada). De acuerdo con la invención, el dispositivo 1120 convencional de servocomando de comparación está, junto con un dispositivo, 1110 de programación de transmisión, dispuesto para formar unos comandos C1 y C2 de control hacia otros nodos. En la práctica, el dispositivo 1110 de programación, el dispositivo 1120 de servocomando de comparación y el dispositivo 1130 de servocomando de conmutación se llevan generalmente a la práctica como un software ejecutado en una unidad de procesamiento de datos, como por ejemplo una UCP, no ilustrada en la FIG. 1. El dispositivo 1110 de programación de transmisión presenta, de acuerdo con la invención, un programa de transmisión almacenado que define los intervalos de transmisión al menos para el nodo A y, de modo preferente, también para otros nodos de control, por ejemplo el nodo B 120. De modo preferente, el programa de transmisión almacenado en el dispositivo 1110 de programación de transmisión define unos intervalos de tiempo de transmisión de TDMA para todos los nodos 110, 120, 130 de control y, posiblemente también, para los servonodos 140, 150, pero existen muchas posibilidades. El dispositivo 1110 de programación de transmisión comprende una base de tiempo sincronizada convencional, esto es, un reloj, no ilustrado, para la definición precisa del programa de transmisión de los nodos 110, 120, 130, 140, 150, esto es, los intervalos de tiempo de TDMA específicos de los nodos. El nodo A 110 comprende un dispositivo transceptor convencional, ilustrado por el dispositivo 1140 receptor y un dispositivo 1150 transmisor en la FIG. 1, conectados al bus 105. El dispositivo 1160 de vigilancia del circuito de guarda puede ser un dispositivo 1160 convencional de vigilancia del dispositivo de guarda que normalmente se lleva a la práctica por medio de un circuito detector de hardware que normalmente lee los impulsos procedentes de la UCP, y puede estar dispuesto para emitir una señal “0” lógica si detecta que el nodo A 110, esto es, su UCP, está funcionando incorrectamente, por cualquier razón, y emitir una señal “1” lógica en caso contrario. Existen muchas posibilidades, el circuito de guarda 1160 puede, de manera opcional, ser alimentado y controlado también por el dispositivo de vigilancia, por el dispositivo 1120 de servocontrol de comparación, como se ilustra en la FIG. 1. La salida del dispositivo 1160 de vigilancia de circuito de guarda está, de acuerdo con la invención, conectado a la entrada de un circuito 1180 de “parlamento electrónico”, aquí designado como dispositivo 1180 de control de acceso de transmisión por bus que aquí está implementado como una puerta AND. Dicho circuito de parlamento electrónico, esto es, un circuito capaz de tomar decisiones y de emitir una/s señal/es de control de salida de acuerdo con ello es convencionalmente designado como un comparador. El dispositivo 1160 de vigilancia de circuito de guarda controla también, de acuerdo con la invención, las señales C1 y C2 de control de salida, como se ilustra en la FIG. 1. Como se ilustra en la FIG. 1, el circuito 1180 es también alimentado por un dispositivo 1170 de “suministro correcto de energía” el cual puede llevarse a la práctica por medio de un circuito de guarda de energía convencional capaz de emitir una señal “bajo” (o “Falso”) tan pronto como el nodo 110 no esté siendo energizado adecuadamente y emitir una señal “alto”, en caso contrario. La puerta 1180 AND controla la transmisión del nodo A 110 sobre el bus 105 mediante el control de un conmutador el cual o bien conecta la vía de transmisión del nodo A 110 con el bus 105 o lo aísla del bus, como se ilustra en la FIG. 1. De acuerdo con la invención, los nodos 110, 120 y 130 están físicamente conectados entre sí por al menos un enlace de comunicación, por ejemplo un circuito 1200, 1210, 1220, 1230, de entrada, que esté físicamente separado del bus de datos. Este/os enlace/s 1200, 1210, 1220, 1230 de transmisión de datos externo que está(n) separado(s) físicamente del bus, pueden llevarse a la práctica por medio de un circuito eléctrico, por ejemplo en forma de cable, hilo, fibra óptica, o línea de entrada de un material eléctricamente conductor, un enlace de radiocomunicación, por ejemplo un enlace inalámbrico Bluetooth™, un enlace de comunicación infrarrojo, un enlace de transmisión de datos por sonar, o combinaciones apropiadas de estos dependiendo del entorno / aplicación. En la forma de realización

ilustrada en la FIG. 1, las señales de salida procedentes del dispositivo 1110 de programa, junto con las señales de salida procedentes del dispositivo 1120 de servocomando de comparación son habilitados a través de las puertas 1300 y 1310 AND, respectivamente, la señal de salida procedente del dispositivo 1160 de vigilancia del circuito de guarda es habilitada junto con la señal de salida procedente del dispositivo 1170 de suministro correcto de energía a través de la puerta 1410 NAND. La señal de salida procedente de la puerta 1410 NAND es habilitada, junto con la señal de salida procedente de la puerta 1300 AND y la señal de salida procedente de la puerta 1310 AND, respectivamente, a través de las respectivas puertas 1420 y 1430 OR de transmisión, como se ilustra en la FIG. 1. Las puertas 1420 y 1430 OR están conectadas a un respectivo dispositivo de control de transmisión por bus correspondiente (no ilustrado) del nodo B 120 y del nodo C 130, por medio de puertas similares OR (no ilustradas). La finalidad de ello es que un nodo de funcionamiento incorrecto no afecte / influencie las transmisiones de nodos de funcionamiento correcto.

De manera similar, el correspondiente dispositivo 1180 de control de acceso de transmisión por bus del nodo A 110 es de acuerdo con la invención alimentado por las señales C3 y C5 de control procedentes del nodo B 120 y del nodo C 130, por medio de una puerta 1440 OR, como se ilustra en la FIG. 1. De esta manera, el diseño del nodo A 110 del nodo B 120 y del nodo C 130 es básicamente el mismo en este ejemplo ilustrativo. Cada nodo puede implementar la funcionalidad software por medio de un software similar con el fin de obtener una diversidad de integridad relativa a los fallos sistemáticos, de una manera convencional. Así, el dispositivo 1110 de programa de transmisión, el dispositivo 1160 de vigilancia del circuito de guarda, la computación del dispositivo 1130 de servocomando y el dispositivo 1120 de servocomando de comparación del nodo A 110 forman conjuntamente un mecanismo de guarda de bus que suprime un comportamiento de transmisión defectuosa del nodo A 110. De manera similar, el nodo B 120 de control y el nodo C 130 de control incorporan unos correspondientes mecanismos de guarda de bus. Debe hacerse hincapié en que el mecanismo de guarda de bus de acuerdo con la invención, en contraste con los guardas de bus convencionales, no solo suprime el comportamiento de la palabrería sin sentido de un sistema de nodo / sino que también potencia el comportamiento de fallo silente del sistema del nodo / bus. Este mecanismo de guarda de bus, está, de acuerdo con la invención, dispuesto para recibir y ser controlado por unas señales C3 y C5 de control entrantes, y para formar y emitir las señales C1 y C2 de salida hacia otro/s nodo/s.

A continuación, con referencia a las FIGS. 1 - 2 y a la tabla inferior que ilustra un ejemplo de transmisiones de datos sobre el bus (105) durante el uso, se describirá con mayor detalle la funcionalidad del sistema 100 de datos de tolerancia de fallos de acuerdo con la invención.

C1	**Falso**	**Falso**	**Verdadero**	**Falso**	**Falso**	**Verdadero**	**Falso**	**Falso**	**Verdadero**
C2	**Falso**	**Verdadero**	**Falso**	**Falso**	**Verdadero**	**Falso**	**Falso**	**Falso**	**Falso**
C3	**Verdadero**	**Falso**	**Falso**	**Verdadero**	**Falso**	**Falso**	**Verdadero**	**Falso**	**Falso**
C4	**Falso**	**Falso**	**Verdadero**	**Falso**	**Falso**	**Verdadero**	**Falso**	**Falso**	**Verdadero**
C5	**Verdadero**	**Falso**	**Falso**		**Falso**	**Falso**	**Verdadero**	**Falso**	**Falso**
C6	**Falso**	**Verdadero**	**Falso**	**Falso**	**Verdadero**	**Falso**	**Falso**	**Falso**	**Falso**

BUS DE DATOS	**S1 = 5,0** **S2 = 4,0**	**S1 = 5,1** **S2 = 3,9**	**S1 = 5,1** **S2 = 4,1**	**S1 = 5,1** **S2 = 4,1**	**S1 = 3,3** **S2 = 4,0**	**S1 = 5,0** **S2 = 4,0**	**S1 = 5,0** **S2 = 4,0**	**No transmisión**	**S1 = 5,1** **S2 = 4,1**
Nodo de transmisión	**A**	**B**	**C**	**A**	**B**	**C**	**A**	**B**	**C**
Intervalo de tiempo	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**

Tabla 1

En la tabla 1, los intervalos 1 a 9 de tiempo representan intervalos de tiempo consecutivos y la tabla 1 puede, por tanto, ser leída como incorporando una línea de tiempo asociada con ella, como si fuera de izquierda a derecha.

El nodo A 110 de control está dispuesto para emitir dos señales, C1 y C2 de control en la tabla 1 y en la FIG. 1, indicativas de si el nodo A 110 permite que el nodo B 120 y / o el nodo C transmitan datos sobre el bus 105. De manera similar, el nodo B 120 y el nodo C 130 están dispuestos para emitir las señales C3 y C5 de control, respectivamente, hacia el nodo A 110. Como se ilustra en la FIG. 1, las señales C1 y C2 pueden ser comunicadas a través del enlace 1210 y 1200, respectivamente, de transmisión de datos, y las señales C3 y C5 de control pueden

ser comunicadas a través del enlace 1230 y 1220, respectivamente, de transmisión de datos. La señal C4 de control de la tabla 1 (no ilustrada en la FIG. 1) es una señal de control enviada desde el nodo B 120 hasta el nodo C 130 y es de manera similar indicativa de si el nodo B 120 permite que el nodo C 130 transmita datos sobre el bus o no. la señal C6 de control de la tabla 1 (no ilustrada en la FIG. 1) es una señal de control enviada desde el nodo C 130 hasta el nodo B 120 y es de manera similar indicativa de si el nodo C 130 permite que el nodo B 120 transmita datos sobre el bus o no. El valor "Verdadero" para, respectivamente, C1, C2, C3, C4, C5 y C6, en la Tabla 1, indica que el nodo específico que emite la señal de control permite que el nodo respectivo que emite la señal de control transmita datos sobre el bus. El valor "Falso" indica que la transmisión de datos está prohibida.

Las transmisiones de datos de los respectivos servonodos 140, 150 de la FIG. 1 han sido omitidos en la Tabla 1, pero una persona experta en la materia comprende que estos servonodos 140, 150 pueden transmitir, por ejemplo en intervalos de tiempo a continuación después de un ciclo de intervalos de tiempo de "comando de control". Por ejemplo, los servonodos 140, 150 pueden estar dispuestos para recibir datos en los intervalos 1 a 9 de tiempo en la Tabla 1 y transmitir sus valores de detección respectivos (retroalimentación) en los siguientes intervalos 10 y 11 de tiempo (no ilustrados en la tabla 1), pero existen muchas posibilidades.

El dispositivo 1120 de servocomando de comparación del nodo A 110 y los dispositivos de servo comando de comparación correspondientes del nodo A 120 y del nodo C 130, leen los servocomandos transmitidos en el respectivo intervalo para el respectivo servo, junto con los correspondientes servocomandos según fueron calculados por su propio nodo (por ejemplo, según fueron calculados por la computación del dispositivo 1130 de servocomando para el nodo A 110) y compara estos comandos entre sí. Si un comando específico se desvía, por ejemplo difiere más de un nivel de umbral fijo o porcentual, respecto, por ejemplo, el valor medio del resto de los comandos, entonces se establece que este comando junto con el nodo específico que calculó / transmitió este comando es inválido / de funcionamiento incorrecto.

Como un ejemplo ilustrativo, si dicho nivel de umbral porcentual se establece en un 10%, y el valor medio para la señal S1 y S2 de control de comando respectivo es calculado de manera continuada sobre la base del intervalo y en base a los datos recibidos en los últimos tres intervalos de tiempo, entonces el dispositivo 1120 de servocomandos de comparación del nodo A 110 calcula este valor medio en 5,05 grados para el servo 1 (S1) y 4,05 grados para el servo 2 (S2), entre el intervalo 5 - 7 de tiempo. El nodo A 110 establece así que el nodo B 120 está funcionado incorrectamente dado que es transmitida una señal de control S1 = 3,3 grados que difiere en más de un 10% de este valor medio calculado (5,05). El nodo A no calcula también sus propios valores de señal de control (S1 = 5,0; S2 = 4,0) en (o inmediatamente antes de) el intervalo 6 de tiempo y transmite estos valores como comandos de control hasta el bus en el intervalo 6 de tiempo.

Dado que el dispositivo 1120 de servocomandos de comparación del nodo A 110 de esta manera ha establecido que el nodo B 120 está funcionando incorrectamente, genera de salida una señal respectiva "Falso" (binario 0) hasta la puerta AND 1300. En consecuencia, la señal C2 de control de salida desciende (binario 0), representada por "Falso" en la tabla 1, dado que la salida desde la puerta NAND 1410 se eleva solo si cualquiera de las salidas procedentes del dispositivo 1170 de suministro correcto de energía y el dispositivo 1160 de vigilancia de circuito de guarda desciende. De manera similar también el valor C6 desciende.

De esta manera, dado que dos señales C2 y C6 de control entrantes en el intervalo 6 de tiempo dicen que el nodo B 120 está funcionando incorrectamente, su dispositivo de control de acceso de transmisión por bus correspondiente al dispositivo 1180 de control de acceso de transmisión por bus del nodo A 110, aísla el conmutador de transmisión del nodo B 120 (correspondiente al conmutador 1155 de transmisión del nodo A 110), y las transmisiones del nodo B 120 están por tanto bloqueadas en el intervalo 8 de tiempo, esto es el nodo B 120, no transmite ningún dato del bus en el intervalo 8 de tiempo. Por tanto, es evidente que la inversión potencia el comportamiento de fallo silente del sistema respectivo de nodo / bus.

Así mismo, dado que C1 - C6 son todas funciones de los programas de transmisión de nodos relevantes, de manera que cualquiera de los valores C1 - C6 desciende tan pronto como el programa de transmisión del intervalo de tiempo de NAND de su nodo emisor desciende (Falso), es evidente que la invención bloquea de manera eficaz las transmisiones de palabrería sin sentido del respectivo sistema de nodo / bus. Esto se ilustra también en la FIG. 2. La FIG. 2 ilustra la manera en que el nodo A 110 está siendo bloqueado para no resultar un nodo de palabrería sin sentido. Como se pone de manifiesto en la FIG. 2, dado que las señales C3, C5 … CN de control descienden todas excepto en el intervalo de tiempo asignado al nodo A 110, el conmutador 1155 del nodo A 110 está siempre en estado de aislamiento excepto durante los intervalos de tiempo asignados al nodo A 110. En consecuencia, ninguna transmisión de "palabrería sin sentido" puede ser transferida sobre el bus 1105.

Aun cuando ha sido descrita con anterioridad una realización de acuerdo con la FIG. 1 en la que el conmutador de transmisión es controlado por, entre otros, 2 señales de control externas y 1 señal de control interna (programa de tiempo del nodo mismo), y en el que el conmutador es bloqueado (esto es puesto en estado de aislamiento) cuando ambas dichas señales de control externo son "Falsas", y es evidente que la invención proporciona una posibilidad de una amplia gama de otras "decisiones mayoritarias" electrónicas para controlar las transmisiones de nodo, esto es, la disposición de conmutador de la FIG. 1 podría estar configurada para aislar solo si solo 3 o más entre, por ejemplo, 4 o más señales de control externo descendieran ("Falsas"). Así mismo, el dispositivo 1180 de control de

acceso de transmisión por bus de la FIG. 1 puede ser llevado a la práctica / configurado para permitir transmisiones sobre el bus incluso en el caso de funcionamiento incorrecto del dispositivo 1110 de programa de transmisión de TDMA, por ejemplo simplemente no dejando que el dispositivo 1110 de programa de transmisión de TDMA se conecte con el dispositivo 1180 de control de acceso de transmisión por bus, y existen muchas posibilidades.

Así mismo, un nodo de control puede estar conectado con un sensor por medio de una interfaz análoga que está separada del bus de datos y en el que el nodo de control está dispuesto para leer valores de muestra procedentes del sensor a través de dicha interfaz análoga. Esto puede ser llevado a la práctica mediante la disposición de un enlace de comunicación convencional, por medio de un puerto de datos dedicado de la UCP del nodo, entre el nodo 110 y un nodo de detección / servo. Esta solución puede ser ventajosa en entornos / aplicaciones en las que un nodo de detección esté alejado de, y no necesariamente necesite comunicar a través del bus, con otros nodos de control pero necesita comunicar con al menos un nodo de control. De esta manera, el nodo de detección en cuanto tal no necesita la protección de la palabrería sin sentido, lo que reduce la complejidad / coste.

Así mismo, la lógica descrita con anterioridad, puede ser llevada a la práctica por medio de cualquier combinación apropiada de hardware / software y la invención no está restringida a los ejemplos ilustrativos que han sido descritos con anterioridad.

Los principios de la presente invención han sido descritos en las líneas precedentes mediante ejemplos de formas de realización o modos / ejemplos de operaciones, esto es en el caso de un sistema de control de vuelo en tiempo real. Sin embargo, como se ha manifestado, la invención es aplicable para cualquier nodo de bus de datos para cualquier sistema de bus de datos (TDMA) de tolerancia de fallos. Por tanto, la invención no debe ser interpretada como limitada a las forma de realización / ejemplos de trabajo concretos analizados con anterioridad, y debe ser apreciado que pueden efectuarse variantes / combinaciones en esas formas de realización / ejemplos de trabajo por las personas expertas en la materia, sin apartarse de la alcance de la presente invención como queda definido por las reivindicaciones adjuntas.

REIVINDICACIONES

1.- Un nodo (110) de bus de datos, que es un nodo (110,120, 130) de control, o un nodo (140, 150) de detección y que está dispuesto para comunicar a través de un bus (105) de datos de Acceso Múltiple por División de Tiempo (TDMA), comprendiendo el nodo (110) de bus de datos:

- un dispositivo (1110) de procesamiento de señal de tiempo que está configurado para definir un programa de transmisión de intervalo de tiempo de TDMA para al menos dicho nodo (110) de bus de datos, el dispositivo (1110) de procesamiento de señal de tiempo está conectado a un dispositivo (1180) de control de acceso a la transmisión por bus por medio de una conexión

- un conmutador (1155) conectado por medio de una conexión al dispositivo (1180) de control de acceso a la transmisión por bus, estando el conmutador (1155) configurado para o bien conectar una vía de transmisión de dicho nodo (110) de bus de datos con el bus (105) o aislarlo de éste y configurado para ser controlado por dicho programa de transmisión de intervalo de tiempo de TDMA para dicho nodo (110) de bus de datos por medio del dispositivo (1180) de control de acceso a la transmisión por bus,

estando dicho nodo (110) **caracterizado porque**

dicho dispositivo (1180) de control de acceso a la transmisión por bus está configurado para ser también controlado por al menos una señal (C3, C5) de control externa, suministrada por al menos otro nodo (120, 130) de bus de datos, por medio de al menos un enlace (1220, 1230) de transmisión de datos externo que está físicamente separado de dicho bus (105), de manera que dicho dispositivo (1180) de control de acceso a la transmisión por bus controla dicho conmutador (1155) por medio de dicha conexión para conectar o aislar dicha vía en base a al menos dicha al menos una señal (C3, C5) de control externa es una función del programa de transmisión de intervalo de tiempo para el nodo (110) de bus de datos, en la que la al menos una señal (C3, C5) de control externa y de un funcionamiento incorrecto detectado de dicho nodo (110).

2.- El nodo (110) de acuerdo con la reivindicación 1, que comprende también un dispositivo (1440) lógico que está configurado para:

- recibir y procesar al menos dos señales (C1, C2) de control de entrada procedentes de una pluralidad de nodos (120, 130) asociados con el bus (105) por medio de dicho/s enlace/s (1220, 1230) de transmisión de datos externos, y

- emitir una señal de control, que es una función de dichas recibidas al menos dos señales de control de entrada, hasta el dispositivo (1180) de control de acceso a la transmisión por bus.

3.- El nodo (110) de acuerdo con la reivindicación 2, en el que el dispositivo (1180) de control de acceso a la transmisión por bus se lleva a la práctica como un comparador y dicho dispositivo (1140) lógico se lleva a la práctica como un comparador.

4.- El nodo de acuerdo con cualquiera de las reivindicaciones 1 a 3, que comprende también un dispositivo (1160) de vigilancia del circuito de guarda para establecer si el propio nodo (110) está funcionando o no de manera incorrecta y en el que dicho dispositivo (1180) de control de acceso a la transmisión por bus está configurado para ser también controlado por el dispositivo (1160) de vigilancia del circuito de guarda.

5.- El nodo de acuerdo con cualquiera de las reivindicaciones 1 a 4, que comprende también un dispositivo (1170) de suministro correcto de energía para establecer si el propio nodo (110) está siendo energizado de una manera precisa y en el que dicho dispositivo (1180) de control de acceso a la transmisión por bus está configurado para ser también controlado por el dispositivo (1170) de suministro correcto de energía.

6.- El nodo (110) de acuerdo con cualquiera de las reivindicaciones 1 a 5, en el que dicho programa de transmisión de intervalo de tiempo de TDMA define también unos intervalos de transmisión para al menos otro nodo (120, 130, 140, 150) asociado con el bus (105), y el propio nodo (110) está dispuesto para:

- formar una señal (C1, C2) de control de salida que es una función de dicho programa de transmisión de intervalo de tiempo de TDMA y

- para emitir dicha señal (C1, C2) de control hasta al menos otro nodo (120, 130, 140, 150) a través de un enlace (1200, 1210) de transmisión de datos externo que está físicamente separado de dicho bus (105).

7.- El nodo (110) de acuerdo con la reivindicación 6, que comprende también un dispositivo (1120) de vigilancia para vigilar las señales de control transmitidas a través del bus (105) por otros nodos (120, 130) de control o los datos de detección transmitidos a través del bus (105) por los nodos (140, 150) de detección asociados con el bus (105), y en el que el dispositivo (1120) de vigilancia está dispuesto para:

- establecer un estado de funcionamiento incorrecto de un nodo (120, 130, 140, 150) de funcionamiento incorrecto asociado con el bus, en base a dicha vigilancia, y

- emitir una señal de control de bloque de transmisión para bloquear otras transmisiones del nodo de funcionamiento incorrecto en respuesta al estado de funcionamiento incorrecto así establecido del nodo de funcionamiento incorrecto,

y en el que el propio nodo (110) está también configurado para formar dicha/s señal/es (C1, C2) como una función de dicha señal de control de bloque de transmisión.

8.- El nodo (110) de acuerdo con las reivindicaciones 6 o 7, que comprende un dispositivo (1160) de vigilancia de circuito de guarda para establecer si el propio nodo (110) está funcionando o no incorrectamente, y en el que el nodo (110) está configurado para formar dicha señal (C1, C2) de control de salida como una función de la señal de control de salida de vigilancia de guarda emitida por dicho dispositivo (1160) de vigilancia de circuito de muestra e indicativa de si el nodo (110) está funcionando incorrectamente o no.

9.- El nodo (110) de acuerdo con cualquiera de las reivindicaciones 6 a 8, que comprende también un dispositivo (1170) de suministro correcto de energía para establecer si el propio nodo (110) está siendo energizado de manera precisa y en el que el nodo (110) está configurado para formar dicha señal (C1, C2) de control de salida como una función de una señal de control procedente de dicho dispositivo (1170) de suministro correcto de energía.

10.- Un sistema (100) de bus de datos de tolerancia de fallos que comprende al menos dos nodos (110, 120, 130, 140, 150) de bus, que son nodos de control o de detección y que están dispuestos para comunicar a través del bus (105) de TDMA, en el que una pluralidad de dichos nodos (110, 120, 130, 140, 150) comprende cada uno un mecanismo de guarda de bus para suprimir un comportamiento de transmisión defectuoso, **caracterizado porque** dicho sistema comprende un nodo (110) de acuerdo con cualquiera de las reivindicaciones 1 a 9.

11.- El sistema (100) de bus de datos de tolerancia de fallos de acuerdo con la reivindicación 10, en el que al menos dos de dichos nodos (110, 120) están conectados por medio de al menos un enlace (1200, 1210, 1220, 1230) de transmisión de datos que está físicamente separado de dicho bus (105), permitiendo con ello que al menos un mecanismo de guarda de bus de uno de los nodos (120) así conectado emita una señal de control hasta el mecanismo de guarda de bus de otro de los nodos (110) así conectados a través de dicho enlace (1200, 1210, 1220, 1230) de transmisión.

12.- El sistema (100) de bus de datos de tolerancia de fallos de acuerdo con la reivindicación 11, en el que al menos tres de dichos nodos (110, 120, 130) están mutuamente interconectados por medio de unos enlaces (1200, 1210, 1220, 1230) de transmisión de datos que están físicamente separados de dicho bus (105), creando de esta forma un grupo de al menos tres nodos que controlan entre sí el mecanismo de guarda de bus por medio de dichos enlaces (1200, 1210, 1220, 1230) de transmisión de datos.

13.- El sistema (100) de bus de datos de tolerancia de fallos de acuerdo con cualquiera de las reivindicaciones 10 a 12, en el que un nodo de control está conectado con un sensor por medio de una interfaz análoga que está separada del bus de datos y en el que el nodo de control está dispuesto para leer valores de muestra procedentes del sensor a través de dicha interfaz análoga.

14.- El sistema (100) de bus de datos de tolerancia de fallos de acuerdo con cualquiera de las reivindicaciones 10 a 13, en el que dicho/s enlace/s (1200, 1210, 1220, 1230) de transmisión de datos externos que está/n físicamente separado/s del bus (105), se lleva(n) a la práctica como:

- un circuito eléctrico, por ejemplo en cable, hilo, o línea de entrada fabricado por un material eléctricamente conductor,

- un enlace de radiofrecuencia, por ejemplo, un enlace inalámbrico Bluetooth™,

- un enlace de comunicación infrarrojo,

- un enlace de transmisión de datos por sonar,

o una combinación de estos.

15.- Una aeronave, **caracterizada porque** comprende un nodo (110) de bus de datos de acuerdo con cualquiera de las reivindicaciones 1 a 9, o un sistema (100) de datos de tolerancia de fallos de acuerdo con cualquiera de las reivindicaciones 10 a 14.

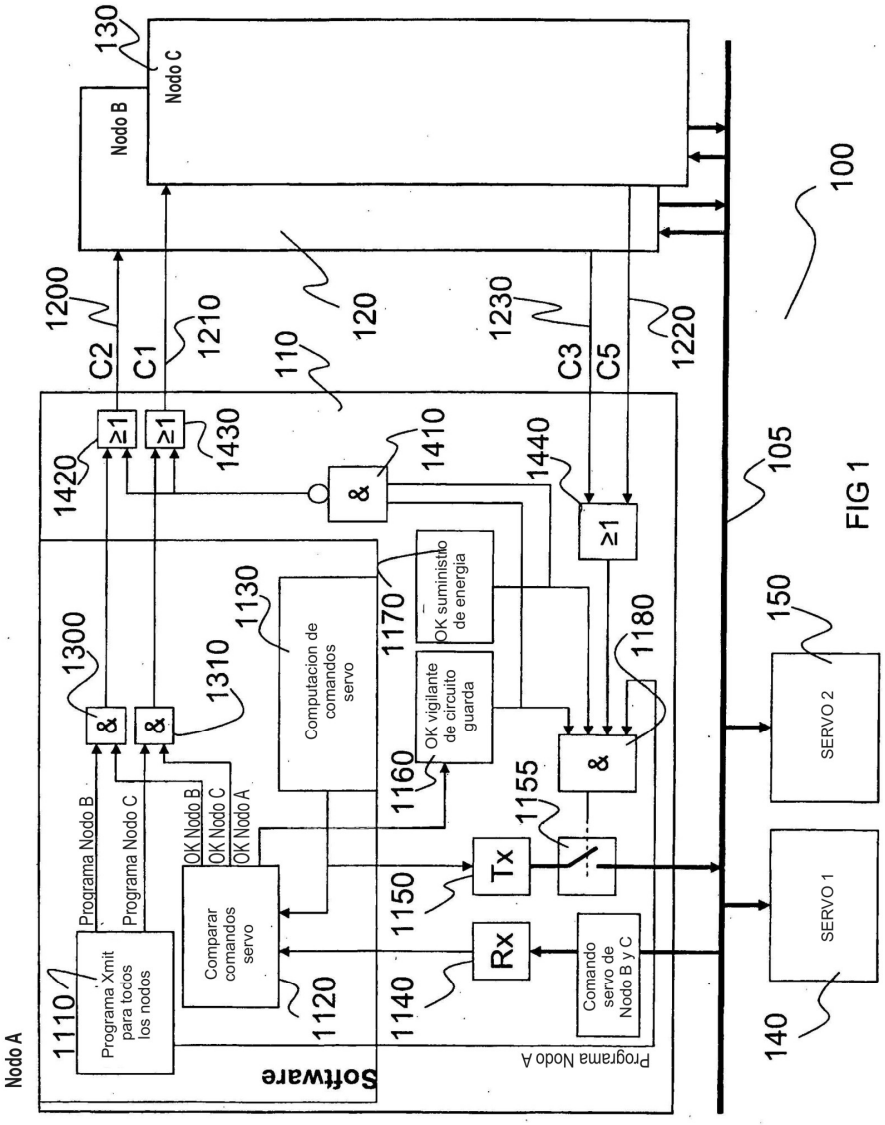
Nodo A
Nodo B
Nodo C
Software
Programa Nodo A
Programa Xmit para todos los nodos
Programa Nodo B
Programa Nodo C
Comparar comandos servo
OK Nodo B
OK Nodo C
OK Nodo A
Computacion de comandos servo
OK vigilante de circuito guarda
OK suministro de energia
Tx
Rx
Comando servo de Nodo B y C
SERVO 1
SERVO 2
C1
C2
C3
C5
1100
1110
1120
1130
1140
1150
1155
1160
1170
1180
1200
1210
1220
1230
1300
1310
1410
1420
1430
1440
105
110
120
130
140
150

FIG 1

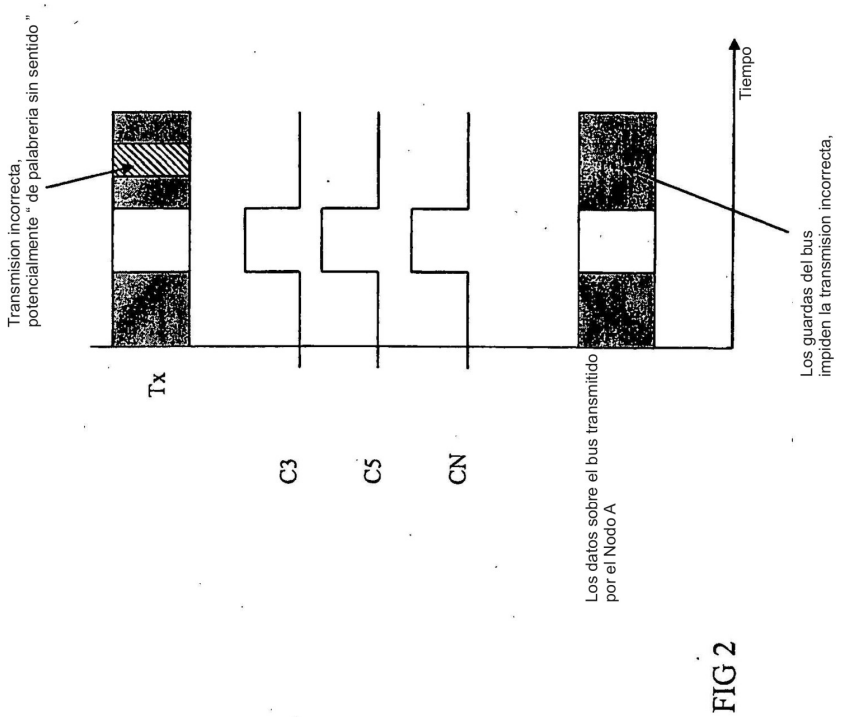
Transmision incorrecta,
potencialmente " de palabreria sin sentido "
Tx
C3
C5
CN
Los datos sobre el bus transmitido
por el Nodo A
Tiempo
Los guardas del bus
impiden la transmision incorrecta,

FIG 2