(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 363 650**

(51) Int. Cl.:
G05B 19/042 (2006.01)
G05B 19/05 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08021860 .5**
(96) Fecha de presentación : **17.12.2008**
(97) Número de publicación de la solicitud: **2075655**
(97) Fecha de publicación de la solicitud: **01.07.2009**

(54) Título: **Control de seguridad.**

(30) Prioridad: **27.12.2007 DE 10 2007 063 291**

(45) Fecha de publicación de la mención BOPI:
11.08.2011

(45) Fecha de la publicación del folleto de la patente:
11.08.2011

(73) Titular/es: **ROBERT BOSCH GmbH**
Postfach 30 02 20
70469 Stuttgart, DE

(72) Inventor/es: **Nikolai, Horst-Dieter y**
Rug, Volker

(74) Agente: **Carvajal y Urquijo, Isabel**

DESCRIPCIÓN

Control de seguridad

La presente invención parte del campo de la técnica de automatización, en particular del campo de los controles programables, en particular el campo de los controles de seguridad, y describe un dispositivo para la elevación de la seguridad en procesos de aplicación así como un procedimiento para el funcionamiento de un control de este tipo.

En máquinas herramientas, máquinas de presión y máquinas de embalaje o en aplicaciones de montaje, de manipulación y de robótica, la protección de personas contra movimientos incontrolados de la máquinas es prioritaria. Todos los fabricantes de máquinas deben realizar, en el marco del diseño de sus máquinas, un análisis de amenazas y una evaluación de riesgos. Para el cumplimiento de estos requerimientos muy altos son necesarios los llamados controles de seguridad para el control de las máquinas.

El documento DE 102004018857 A1 muestra un control de seguridad del estado de la técnica. El cometido de la solución descrita aquí consiste en preparar un procedimiento y un dispositivo para el control de funciones de seguridad en el marco de un control del sistema ajustado a funciones de seguridad, de manera que el programa de seguridad que agrupa las funciones de seguridad se caracteriza por una complejidad reducida y se puede ejecutar en entorno de programa inseguro discrecional, sin que errores en el control de funciones de seguridad no relevantes para la seguridad conduzcan a un fallo durante el control de funciones de seguridad.

Los procesos de aplicación en conexión con controles de seguridad son realizados, en general, por medio de un control propiamente dicho y por una pluralidad de aparatos de campo. El cometido de los aparatos de campo es detectar y supervisar los estados de procesos y transmitir estas informaciones relevantes para el proceso al control o recibir informaciones relevantes del proceso desde el control. Los aparatos de campo pueden ser, por ejemplo, sensores, pulsadores, avisadores de movimiento, pero también accionamientos eléctricos. La conexión entre el aparato de campo y el control se realiza, por ejemplo, por medio de los llamados medios de entrada y de salida (módulos de entrada / salida). Los módulos de entrada y salida se pueden comunicar con el control, por ejemplo, por medio de un bus de campo. Los módulos de entrada y salida pueden estar ordenados jerárquicamente y se conectan, en general, por medio de una llamada cabeza de bus de campo en el bus de campo. A un control seguro pertenecen también módulos de entrada y de salida seguros.

Actualmente, la Firma Solicitante ha adquirido en el mecano bajo la designación SERCOS Interface® (SErial Real Time COmmunication System) un sistema de comunicaciones distribuido con estructura de forma anular, que es adecuado como bus de campo para aplicaciones de seguridad, pero que no está prescrito obligatoriamente. Los usuarios están conectados aquí normalmente por medio de guías de ondas ópticas con un usuario central (por ejemplo, el control). El sistema SERCOS Interface® especifica una comunicación estrictamente jerárquica. Los datos son intercambiados en forma de bloques de datos, los llamados telegramas o “Cuadros” (Frames) en ciclos de tiempo constante entre el control (maestro) y las subestaciones (subordinado). No tiene lugar una comunicación directa entre los otros usuarios o bien las subestaciones. Adicionalmente se establecen contenidos de datos, es decir, que la importancia, representación y funcionalidad de los datos transmitidos está en gran medida predefinidos. En el sistema SERCOS Interface®, al maestro corresponde la activación del control en el anillo y al subordinado corresponde la conexión de una o varias subestaciones (accionamientos o módulos de entrada y salida). Son posibles varios anillos en un control, siendo la coordinación de los anillos individuales entre sí una tarea del control y no es especificada por el sistema SERCOS Interface®. Normas de bus de campo alternativas serían Profibus o CAN-Bus.

La condición previa básica para componentes de una aplicación de seguridad es que éstos adopten un estado seguro en el caso de una avería de funcionamiento. Por un estado seguro se entiende aquel estado, que impide con seguridad una amenaza potencial. Para el campo de la técnica de automatización, en general, el estado libre de energía es un estado seguro. Para la comunicación se utiliza en estas aplicaciones los llamados buses de campo seguros, que se pueden basar, por ejemplo, en el sistema SERCOS Interface® descrito anteriormente. Los componentes relevantes para la seguridad deben cumplir, además, las normas competentes, como la IEC 61508 y son certificados por centros de certificación, como por ejemplo el TÜV. Además, existen diferentes niveles de seguridad SIL 1-4, a los que se pueden asociar estos módulos.

Los controles conocidos a partir del estado de la técnica trabajan, en general, con al menos un medio de procesamiento de datos para la realización de al menos dos canales de datos así como con preferencia con una derivación de datos, por medio de la cual confluyen los dos canales de datos y pueden ser depositados en un medio de memoria. Los datos se pueden depositar también sin la utilización de una derivación en una memoria y a continuación se puede verificar su corrección. Una unidad de procesamiento de datos de orden superior puede acceder entonces a la memoria y puede leer los datos. En la unidad de procesamiento de datos de orden superior se trata, en general, de un sistema Host, por ejemplo un sistema de bus de campo (Profibus, SERCOS, etc.).

Los principios conocidos a partir del estado de la técnica para la realización de controles de seguridad pueden ser propensos a fallos y, por lo tanto, representan un riesgo para la seguridad, cuando es posible un acceso al medio de

memoria en cualquier momento y de forma incontrolada. Es decir, que independientemente de si los datos están presentes completos o correctos en el medio de memoria, se podría realizar un acceso a datos teóricamente incompletos y, por lo tanto, inseguros. El documento EP-A-1 672 446 y el documento EP-A-1 128 241 describen, respectivamente, un control de acuerdo con el preámbulo de la reivindicación 1.

El cometido de la invención consiste en elevar adicionalmente la seguridad de controles de seguridad.

La invención soluciona este cometido con el control de acuerdo con la reivindicación 1 y con el procedimiento de acuerdo con la reivindicación 12. En este caso, el cometido se soluciona utilizando un control con al menos un medio de procesamiento de datos para la realización de un primer canal de datos y de un segundo canal de datos así como con un medio de transmisión de datos o bien con una memoria de transferencia, que está conectada con los dos canales de datos de tal forma que a través del medio de transmisión de datos se pueden transmitir datos desde al menos un canal de datos a una instalación o bien sistema Host o bien Host de orden superior que está conectado en el control, de manera que de acuerdo con la invención está previsto un bloqueo activo de datos o bien un bloqueo activo de Host, por medio del cual se puede ejercer una influencia sobre la transmisión de datos, que puede ser realizada a través del medio de transmisión de datos, a la instalación de orden superior.

En el medio de transmisión de datos se trata de una unidad de cálculo (microcontrolador, CPU), que puede realizar al mismo tiempo varios canales de datos (en tiempo real). Evidentemente, también se podrían utilizar varias unidades de cálculo en paralelo, que están realizadas sobre el mismo silicio o se pueden constituir por separado. La realización concreta depende de la aplicación y del volumen futuro de datos. La solución de acuerdo con la invención tiene la ventaja de que se puede realizar una transmisión de datos a la instalación de orden superior en un instante definible y la instalación de orden superior solamente recibe un derecho de acceso cuando los datos a leer son válidos. La solución de acuerdo con la invención se puede emplear en conexión con todos los protocolos disponibles (SERCOS, Profibus, etc.), aunque entonces el protocolo seguro a transmitir se base, por ejemplo, en un número impar de bytes. Con la idea de acuerdo con la invención se evitan accesos en colisión al medio de transmisión de datos a través de accesos de datos por medio de varias instancias (unidad de cálculo, instalaciones de orden superior, canales) y se puede controlar la transmisión de datos, lo que facilita especialmente el cumplimiento de las especificaciones de centros de certificación para aplicaciones relevantes para la seguridad. La invención se puede realizar, por ejemplo, como SPS de varios canales y autónomo o como módulo de seguridad que cumple la función de un control de seguridad en conexión con otros componentes de la técnica de accionamiento (regulador del accionamiento, control del accionamiento, SPS, NC, etc.) como unidad que trabaja de forma antártica independientemente de la función de los otros componentes. La invención se puede realizar también como módulo opcional para periferia específica del accionamiento, cuya función se puede conectar con la función de la periferia. En la unidad de orden superior, o bien en el sistema de orden superior, se podría tratar, por ejemplo, de un sistema de bus de campo (sistema Host), que intercambia datos de proceso en serie o de manera opcional según la aplicación también en paralelo entre el control de acuerdo con la invención y, por medio del sistema de bus, actuadores y/o sensores conectados en el control. Por medio de la invención es posible interrumpir el intercambio de datos con actuadores y/o sensores en el caso de la presencia de telegramas falsos o incompletos, que sirven para el encapsulamiento de los datos de proceso, y realizar un bloqueo controlable activamente de la transmisión de los datos. Al mismo tiempo de esta manera se suprimen de manera efectiva ventanas de tiempo con estados de datos indefinidos, lo que impide el procesamiento posterior de datos no válidos a través de la periferia de control y previene riesgos para la seguridad.

El procedimiento para el funcionamiento de un control mencionado anteriormente comprende las siguientes etapas del procedimiento:

> Procesamiento de datos (redundante) a través del medio de procesamiento de datos o bien por medio de canales de datos autárquicos que existen en paralelo entre sí, que pueden estar realizados por medio de uno o varios medios de procesamiento de datos; transmisión de datos (redundante) por medio de los canales de datos al medio de transmisión de datos utilizando buses de direcciones y buses de datos paralelos independientes entre sí; influencia del flujo de datos entre los canales y/o una unidad de orden superior que se puede conectar teniendo en cuenta una señal de liberación de datos, que puede activar o desactivar el bloqueo de datos. Por medio del bloqueo de datos se pueden transmitir datos bidireccionalmente, activando el bloqueo de datos por medio de una señal de control. Sobre el medio de transmisión de datos se realizan al mismo tiempo varios accesos de lectura por medio de los canales, de manera que por medio de los canales se pueden transmitir datos de forma redundante a los medios de transmisión de datos.

Las formas de realización ventajosas de la invención se deducen a partir de las reivindicaciones dependientes. De manera más ventajosa, al menos uno de los canales utiliza una interfaz física de datos para el intercambio de datos con el medio de transmisión de datos, que es la misma interfaz física de datos, que utiliza el medio de transmisión de datos para el intercambio de datos con el bloqueo de datos. Esto ahorra líneas de datos adicionales o bien buses de datos.

Con preferencia, el control de la transmisión de datos se realiza por medio de una señal de liberación de datos, que se puede realizar también a través del medio de proceso de datos. La transmisión de datos se puede supervisar de esta manera a través del medio de procesamiento de datos o bien teniendo en cuenta un resultado de la verificación generado a través del medio de procesamiento de datos.

El control de la transmisión de datos por medio de la señal de transmisión de datos se puede realizar adicionalmente también todavía teniendo en cuenta un medio de supervisión controlable en el tiempo. En función del resultado de la supervisión se realiza una transmisión de datos o un bloqueo de datos. Con preferencia se enlazan lógicamente entre sí varios criterios de decisión, para realizar una transmisión de datos o un bloqueo de datos. Por ejemplo, varios canales realizados a través del medio de procesamiento de datos podrían realizar medidas de supervisión separadas con respecto a la fiabilidad y la seguridad de datos transmitidos, siendo realizado por medio de un enlace-Y lógico una liberación de datos solamente cuando la verificación, por ejemplo, por medio de todos los canales y a través del medio de verificación tendría como consecuencia un resultado positivo.

Con preferencia, el medio de transmisión de datos está realizado a través de un medio de memoria, sobre el que son posibles al mismo tiempo varios accesos de lectura y/o accesos de escritura. De esta manera se posibilita una transmisión redundante y paralela de datos idénticos desde el medio de procesamiento de datos (canales) a los medios de transmisión de datos, pudiendo activarse el bloqueo de datos también teniendo en cuenta un proceso de transmisión de datos a una instalación de orden superior que se puede conectar.

El bloqueo de datos se realiza con preferencia por medio de un control de bus de datos que trabaja de forma bidireccional, que se puede controlar por medio de una lógica de control interna y está dispuesto entre el medio de transmisión de datos y la instalación de orden superior conectable. Tales módulos posibilitan una realización económica de la idea de acuerdo con la invención, porque aquí se trata de productos en masa que se pueden adquirir en grandes números de piezas.

De manera muy especialmente preferida, está previsto un medio de ensayo realizado por medio de una señal de retorno, por medio del medio se puede verificar la capacidad funcional del bloqueo de datos. El medio de ensayo se puede activar con preferencia a través del medio de procesamiento de datos y, por lo tanto, por medio de los canales realizados de forma autárquica entre sí o por medio de al menos unote los canales. De esta manera, la lógica del canal puede verificar, antes de la emisión de datos, de forma automática, la funcionalidad correcta del bloqueo de datos. Evidentemente, el medio de ensayo podría ser verificable también por medio de una instalación adicional comprenda por el control o a través del medio de supervisión controlable en el tiempo, que podría comprender también funciones lógicas (microcontrolador). Con preferencia, en particular durante la inicialización del control, debería verificarse la función del bloqueo de datos.

De manera opcional, también podrían estar comprendidos más de dos canales de datos, por ejemplo tres o cuatro canales, que trabajan igualmente de forma autárquica entre sí y que están realizados a través del medio de procesamiento de datos o a través de varios medios de procesamiento de datos. Por lo tanto, de esta manera sería posible transmitir protocolos, en los que la anchura de datos transmitida es n x 8 bits o n x 16 bits o n x 32 bits con n = 1, 2, 3, etc. (n = número par), de tal manera que un canal transmite en cada caso un byte o un byte doble o 32 bits, siendo agrupados estos datos a continuación a través del medio de transmisión de datos y, dado el caso, por medio de la unidad de orden superior conectable de nuevo en un protocolo seguro.

Con preferencia, el control de seguridad de acuerdo con la invención está realizado como módulo de enchufe para un PC de la industria, que posibilita un control en tiempo real independientemente de la periferia del PC. Cada PC se puede equipar de esta manera de forma económica para el SPS de seguridad. La conexión al hardware del PC podría realizarse por medio de la interfaz PCl o por medio de otras interfaces PC conocidas.

De manera alternativa, el control de acuerdo con la invención podría estar comprendido también por una instalación de regulación del accionamiento, con lo que se obtiene una combinación de un control de accionamiento y una regulación de accionamiento, que se puede aplicar para aplicaciones críticas de la seguridad y es especialmente compacta.

Además, de manera alternativa, también sería posible ampliar un SPS estándar con un control de seguridad de acuerdo con la invención, que está realizado, por ejemplo, como módulo de enchufe para un SPS estándar. La funcionalidad SPS estándar existente como anteriormente podría utilizarse, por lo tanto, para procesos no críticos para la seguridad, mientras que en paralelo o de forma totalmente autárquica o teniendo en cuenta ciclos estándar implementados sería posible un funcionamiento seguro de módulos de entrada y salida.

Con preferencia, por medio de la invención se realiza una disposición para la activación segura de módulos de entrada y salida, que comprende al menos uno de los dispositivos de acuerdo con la invención mencionados anteriormente, estando prevista entre el dispositivo y los módulos de entrada y salida a controlar con seguridad una unidad de orden superior, por medio de la cual se pueden transmitir datos entre el dispositivo y los módulos seguros de entrada y salida por medio de la utilización de un protocolo seguro de datos. La figura 1 muestra una disposición de acuerdo con la invención para el bloqueo de telegramas falsos o incompletos dirigidos a la seguridad por medio

de un bloqueo de Host. Esta disposición comprende un lado A relevante para la seguridad y un lado B no relevante para la seguridad. Las operaciones que se realizan en el lado A requieren medidas especiales, de manera que no se pueden producir riesgos agravantes para la seguridad durante el funcionamiento de una instalación accionada por medio de un control. Las operaciones que se realizan en el lado B se limitan a la transmisión de datos asegurados por medio de un protocolo seguro. El lado B se designa también como canal gris. El canal gris está dispuesto, entre otras cosas, entre interfaces de entrada y salida seguras a activar y el control de seguridad.

El control de seguridad mostrado en la figura 1 comprende un vigilante (Watchdog) 9 que se puede conectar opcionalmente, un primer canal 1, un segundo canal 2, un tercer canal opcional 7, buses de direcciones bidireccionales y/o buses de datos (dobles flechas negras), un medio de transmisión de datos o bien una memoria de transmisión 3 (por ejemplo, Dualport RAM, Triport RAM de acuerdo con el número de los canales 1, 2, 7), una instalación de orden superior o bien un sistema Host 5 (bus de campo, etc.), un bloqueo de datos o bien bloqueo de Host 4, una puerta-Y & con señal de salida 6, así como un medio de ensayo, que está realizado por medio de una o varias señales de retorno 8 con Pull up hacia Vcc sobre el lado relevante para la seguridad A y una conexión GND en el lado B no relevante para la seguridad.

En el medio de transmisión de datos 3 se depositan los telegramas dirigidos a la seguridad, generados por el control de seguridad (asegurados a través de un protocolo de seguridad) por medio de los canales 1, 2, 7. Puesto que durante esta fase de la deposición de los datos podrían acumularse telegramas incompletos o erróneos o no verificados en el medio de transmisión de datos 3, se bloque en primer lugar el acceso de la instalación 5 de orden superior a los medios de transmisión de datos 3 por medio del bloqueo de datos 4. Solamente cuando los canales o bien los canales de datos 1, 2, 7 individuales han verificado los mensajes seguros de salida en el medio de transmisión de datos 3, se libera el acceso de la instalación 5 de orden superior a los medios de transmisión de datos 3 por medio del bloqueo de datos 4. Cada canal 1, 2, 7 individual debe conceder explícitamente su conformidad, para que se libere el bloqueo de datos 4, con lo que se suprimen “vacíos” temporales, durante los cuales se podrían leer telegramas “inseguros” a través de la instalación 5 de orden superior. El bloqueo de datos 4 propiamente dicho está constituido por controles de buses de datos bidireccionales y por controladores de direcciones unidireccionales y se puede activar por medio de la señal de control 6. Adicionalmente, en este ejemplo de realización, un vigilante 9 discreto (por ejemplo, un microcontrolador para la supervisión temporal y lógica del programa de los canales 1, 2, 7) debe conceder su conformidad, para que se libere el bloqueo de datos 4. En caso de errores de la supervisión de la ejecución temporal y lógica del programa de los canales 1, 2, 7, esto es detectado por el vigilante 9 discreto y activa de manera duradera el bloqueo de datos 4, de manera que no se pueden lee telegramas nuevos por la instalación 5 de orden superior desde el medio de transmisión de datos 3. La señal de control 6 es suministrada en este ejemplo por una puerta 6, que enlaza los resultados de la verificación de los canales 1, 2, 7 y del vigilante 9 lógicamente entre sí, de tal manera que solamente resulta una señal de control 6 cuando todos los ensayos de verificación se desarrollan de forma positiva.

La posibilidad de ensayo de la funcionalidad del bloqueo de datos 4 se garantiza a través de una o varias señal(es) de retorno 8. Esta(s) señal(es) de retorno 8 está(n) constituida(s), por ejemplo, por uno o varios bits del controlador del bus de direcciones del bloqueo de datos 4, que se han conectado entre GND y un Pull up R y cuyo potencial se puede consultar por medio de los canales 1, 2, 7 o bien de la instalación de procesamiento de datos para la realización de los canales 1, 2, 7.

El cierre / bloqueo de la transmisión de datos de salida (protocolo de seguridad) se realiza en virtud de la invención directamente en el lugar de transmisión hacia la instalación 5 de orden superior (por ejemplo, bus de campo). Solamente cuando está disponible un protocolo ensayado válido, se libera la transmisión de datos, El vigilante 9 representa una segunda vía de desconexión, que eleva adicionalmente la seguridad. Un empleo de este concepto de acuerdo con la invención en forma de un módulo se podría emplear en las más diferentes variantes de controles (solución Rack, solución PC, etc.). La invención convierte un control estándar en un control de seguridad de varios canales.

REIVINDICACIONES

1.- Control con al menos un medio de procesamiento de datos para la realización de un primer canal de datos (1) y de un segundo canal de datos (2), con un medio de transmisión de datos (3), que está conectado con ambos canales de datos (1, 2), de tal manera que a través del medio de transmisión de datos (3) se pueden transmitir datos desde al menos un canal de datos (1, 2) a una instalación de orden superior conectada en el control, y con un bloqueo de datos activo (4), por medio del cual se puede ejercer una influencia sobre la transmisión de datos realizada a través del medio de transmisión de datos a la instalación de orden superior (5), caracterizado porque el medio de transmisión de datos (3) está realizado a través de un medio de memoria, al que son posibles varios accesos al mismo tiempo, en el que la transmisión de datos realizada a través del medio de transmisión de datos (3) a la instalación de orden superior (5) se puede influenciar por medio del bloqueo de datos (4), de tal manera que la instalación (5) de orden superior solamente recibe un derecho de acceso a datos memorizados en el medio de transmisión de datos (3) cuando cada uno de los dos canales de datos (1, 2) ha concedido explícitamente su conformidad para la liberación del bloqueo de datos (4).

2.- Control de acuerdo con la reivindicación 1, en el que al menos un canal de datos (1, 2) utiliza una interfaz física de datos para el intercambio de datos con el medio de transmisión de datos (3), que es la misma interfaz física de datos que utiliza el medio de transmisión de datos (3) para el intercambio de datos con el bloqueo de datos (4).

3.- Control de acuerdo con una de las reivindicaciones anteriores, en el que la influencia sobre la transmisión de datos se realiza por medio de una señal de liberación de datos (6), que se puede generar también a través del medio de procesamiento de datos.

4.- Control de acuerdo con una de las reivindicaciones anteriores, en el que la influencia sobre la transmisión de datos se realiza por medio de una señal de liberación de datos (6), que se puede generar también a través de un medio de supervisión (9) controlable en el tiempo.

5.- Control de acuerdo con una de las reivindicaciones anteriores, en el que el bloqueo de datos (4) está realizado por medio de un control del bus de datos que trabaja bidireccionalmente, y que se puede controlar por medio de una lógica de control interna y está dispuesta entre el medio de transmisión de datos (3) y la instalación (5) de orden superior conectable por medio de al menos un bus.

6.- Control de acuerdo con una de las reivindicaciones anteriores, en el que está previsto un medio de ensayo, que está realizado por medio de una señal de retorno (8) , por medio de la cual se puede verificar la capacidad funcional del bloqueo de datos (4).

7.- Control de acuerdo con una de las reivindicaciones anteriores, en el que están comprendidos más de dos canales de datos (1, 2, 7).

8.- Control de acuerdo con una de las reivindicaciones anteriores, en el que este control está realizado como módulo de enchufe para un PC de la industria.

9.- Control de acuerdo con una de las reivindicaciones anteriores, en el que este control está comprendido por una instalación de regulación del accionamiento.

10.- Control de acuerdo con una de las reivindicaciones anteriores, en el que este control está comprendido por un SPS.

11.- Disposición para el control seguro de al menos un módulo de entrada seguro y/o de un módulo de salida seguro, que comprende un control de acuerdo con una de las reivindicaciones 1 a 11, en el que entre el control y el módulo de entrada y/o el módulo de salida está prevista la instalación (5) de orden superior, por medio de la cual se pueden transmitir datos entre el control y el módulo de entrada seguro y/o el módulo de salida seguro por medio de un protocolo de datos seguro.

12.- Procedimiento para el funcionamiento de un control con al menos un medio de procesamiento de datos para la realización de un primer canal de datos (1) y de un segundo canal de datos (2) así como con un medio de transmisión de datos (3), que está conectado con los dos canales de datos (1, 2), de tal forma que a través del medio de transmisión de datos (3) se pueden transmitir datos desde al menos un canal de datos (1, 2) a una instalación (5) de orden superior conectada en el control, en el que está previsto un bloqueo activo de datos (4), por medio del cual se puede ejercer una influencia sobre la transmisión de datos realizable a través del medio de transmisión de datos (3) a la instalación (5) de orden superior, con las siguientes etapas del procedimiento:

a) procesamiento de datos a través del medio de procesamiento de datos;

b) transmisión de datos por medio de los canales de datos (1, 2) al medio de transmisión de datos (2), que está realizado a través de un medio de memoria, al que son posibles varios accesos al mismo tiempo;

c) influencia sobre el flujo de datos para una instalación (5) que se puede conectar en el control, de tal manera que la instalación (5) de orden superior solamente recibe un derecho de acceso a datos memorizados en el medio de transmisión de datos (3) cuando cada uno de los dos canales de datos (1, 2) ha concedido explícitamente su conformidad para la liberación del bloqueo de datos (4).

13.- Procedimiento de acuerdo con la reivindicación 12, en el que el medio de procesamiento de datos genera una señal para la generación de una señal de liberación de los datos (6) teniendo en cuenta un resultado de una verificación de datos transmitidos por medio de los canales de datos (1, 2) al medio de transmisión de datos (3).

14.- Procedimiento de acuerdo con una de las reivindicaciones 12 ó 13, en el que por medio del bloqueo de datos (4) se transmiten datos bidireccionalmente, siendo activado el bloqueo de datos (4) por medio de una señal de liberación de datos (6).

15.- Procedimiento de acuerdo con una de las reivindicaciones 12 a 14, en el que especialmente durante la inicialización del control se verifica la función del bloqueo de datos (4).

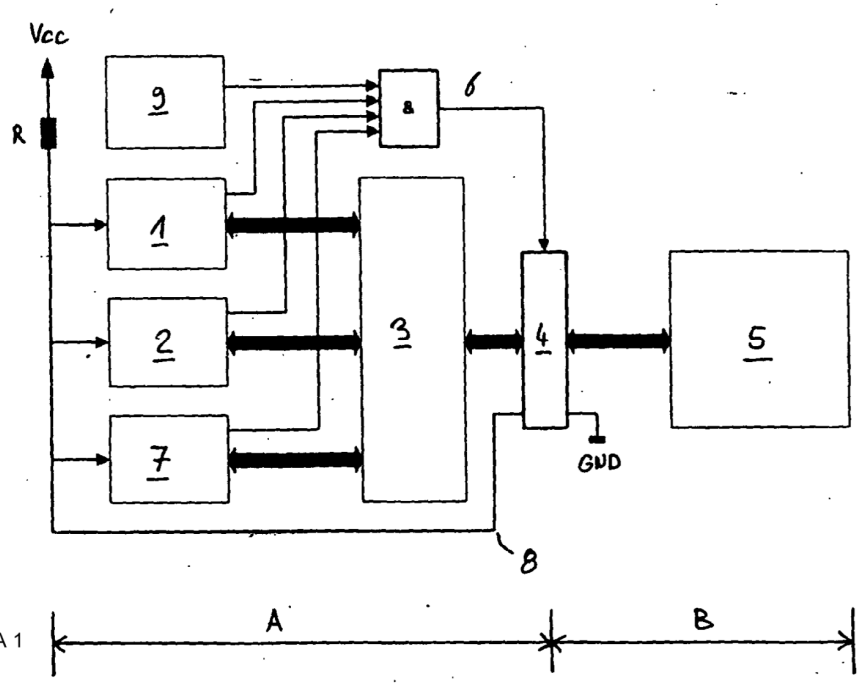

FIGURA 1