(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 010 348**

(51) Int. Cl.:

H04L 43/0817 (2012.01)
H04L 41/0816 (2012.01)
H04L 41/0659 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **05.05.2020 PCT/EP2020/062381**

(87) Fecha y número de publicación internacional: **03.12.2020 WO20239370**

(96) Fecha de presentación y número de la solicitud europea: **05.05.2020 E 20728401 (9)**

(97) Fecha y número de publicación de la concesión europea: **13.11.2024 EP 3977211**

(54) Título: **Sistema de control y procedimiento de funcionamiento de un sistema de control**

(30) Prioridad:

28.05.2019 DE 102019207809

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.04.2025

(73) Titular/es:

SIEMENS MOBILITY GMBH (100.00%)
Otto-Hahn-Ring 6
81739 München, DE

(72) Inventor/es:

GRIEBEL, STEPHAN

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Sistema de control y procedimiento de funcionamiento de un sistema de control

La invención se refiere a un sistema de control y a un procedimiento para operar un sistema de control.

Los sistemas de control, en particular los sistemas de control de sistemas de movilidad, sistemas industriales o sistemas de edificios, suelen comprender un ordenador central (posiblemente multicanal) o una unidad informática para controlar y supervisar uno o varios actuadores del sistema de control u otros componentes del sistema de control con suficiente seguridad. Por regla general, deben respetarse los denominados principios a prueba de fallos (seguridad en caso de fallo) y las medidas para alcanzar y mantener un estado seguro del sistema de control. Se especifican diversas medidas para cumplir dichos principios, por ejemplo, definiendo los denominados niveles de integridad de la seguridad (SIL).

La implementación de ordenadores centrales o unidades informáticas adecuadas dentro de un sistema de control es compleja y costosa, sobre todo para cumplir los requisitos de seguridad descritos con anterioridad.

El documento DE 102 11 279 A1 se refiere a un procedimiento en el que al menos otro ordenador de proceso conectado a un sistema de comunicación comprueba la funcionalidad de al menos un primer ordenador de proceso conectado al sistema y, si se detecta un error, envía un mensaje de control a través del sistema para controlar el primer procesador. Se comprueba si el ordenador de proceso emisor está autorizado a controlar el primer ordenador de proceso y está activo en el sistema de comunicación.

El documento DE 198 26 131 A1 se refiere a un medio para optimizar la fiabilidad y versatilidad en el funcionamiento de un dispositivo de frenado eléctrico para vehículos de motor y comprende una primera unidad que recibe la señal de accionamiento de al menos un actuador de freno accionable por un conductor y determina el valor de consigna para controlar un freno de rueda basándose en la señal de accionamiento, y segundas unidades que se relacionan con el freno de rueda y convierten el valor de consigna en la señal de control para el freno de rueda.

Es tarea de la invención describir un sistema de control y un procedimiento para operar un sistema de control que permita una implementación más simple y con el que, no obstante, se puedan detectar fallos que también puedan ser desencadenados por un comportamiento defectuoso o un mal funcionamiento del componente de control o del componente de monitorización, independientemente de un estado del actuador (o de un fallo dentro del actuador).

Esta tarea se resuelve, según un primer aspecto, mediante un sistema de control de acuerdo con la reivindicación 1 de la patente. Otras realizaciones e implementaciones se describen en las subreivindicaciones asociadas.

El sistema de control presenta al menos un actuador y varios componentes de control. Los componentes de control están configurados para controlar el actuador y generar una primera información de estado. El sistema de control presenta varios componentes de monitorización que están configurados para monitorizar un estado del actuador y generar una segunda información de estado. Además, el sistema de control dispone de una red de comunicación. Los componentes de monitorización y los componentes de control están integrados en la red de comunicación y están configurados para intercambiar la primera y la segunda información de estado entre sí a través de la red de comunicación. Los componentes de monitorización y los componentes de control están configurados para comparar entre sí la primera y la segunda información de estado (intercambiadas). Alternativa o adicionalmente, los componentes del monitor y los componentes de control están configurados para comparar la primera y/o segunda información de estado con información de estado predeterminada.

Tanto el componente de monitorización como el componente de control (en este punto y posteriormente) están configurados para transferir el sistema de control a un estado seguro si una comparación de la primera y segunda información de estado entre sí y/o correspondientemente con la información de estado predeterminada da como resultado una desviación de la primera y segunda información de estado entre sí y/o correspondientemente de la información de estado predeterminada.

Una ventaja del sistema de control aquí descrito es que el control y la monitorización seguros pueden llevarse a cabo mediante una combinación del al menos un componente de monitorización y el al menos un componente de control dentro de la red de comunicación del sistema de control. El componente de monitorización y el componente de control son sencillos y económicos. En comparación con las soluciones convencionales con un ordenador central o una unidad de cálculo central y compleja, el sistema de control del tipo aquí descrito es más sencillo y barato de implementar y sigue garantizando un nivel de seguridad muy elevado. Este nivel de seguridad puede demostrarse en los procedimientos de verificación de la seguridad cumpliendo los requisitos de las normas pertinentes.

Debido a que el componente de control y el componente de monitorización están configurados para generar por separado una primera y una segunda información de estado y para intercambiarlas entre sí a través de la red de comunicación, y debido a que el componente de control y el componente de monitorización están configurados para intercambiar la primera y la segunda información de estado, intercambiaron entre sí la primera y la segunda

información de estado (o individualmente con información de estado predeterminada) (ya sea comparación de la primera y la segunda información de estado en el componente de monitorización y/o comparación de la primera y la segunda información de estado en el componente de control y/o comparación de la primera o segunda información de estado con información de estado predeterminada en el componente de monitorización y/o comparación de la primera o segunda información de estado con información de estado predeterminada en el componente de control) proporciona monitoreo multicanal y/o transferencia del sistema de control a un estado seguro. El hecho de que el sistema de control pueda ser transferido a un estado seguro tanto por el componente de monitorización como por el componente de control cumple un principio a prueba de fallos. De este modo, el sistema de control del tipo aquí descrito es suficientemente seguro en el sentido de que se garantiza una protección adecuada contra fallos tanto sistemáticos como accidentales. De este modo, el sistema de control se diseña de tal manera que cumple un nivel de integridad de la seguridad especialmente elevado. Por ejemplo, puede alcanzarse un nivel de integridad de la seguridad SIL-2, SIL-3 o posiblemente superior de conformidad con la norma EN50129:2018.

Otra ventaja del sistema de control aquí descrito es que puede ampliarse o escalarse muy fácilmente para incluir componentes adicionales. De acuerdo con la invención, el sistema de control presenta un número, en particular una pluralidad k de actuadores, una pluralidad m de componentes de control y una pluralidad n de componentes de monitorización. En particular, una pluralidad de m componentes de control y una pluralidad de n componentes de monitorización permiten una buena escalabilidad para una amplia variedad de aplicaciones, por lo que la interacción de los m componentes de control y los n componentes de monitorización dentro de la red de comunicación permite la redundancia o el control multicanal, la monitorización y la transferencia del sistema de control al estado seguro. Ventajosamente, cada uno de los m componentes de control o cada uno de los n componentes de monitorización está configurado para recibir primera o segunda información de estado de otro u otros de los m componentes de control u otros de los n componentes de monitorización a través de la red de comunicación y para llevar a cabo una comparación de primera y segunda información de estado entre sí o correspondientemente con información de estado predeterminada. Ventajosamente, cada uno de los m componentes de control o cada uno de los n componentes de monitorización está configurado para transferir el sistema de control al estado seguro después de una comparación correspondiente.

El sistema de control reconoce los fallos que se producen de manera sistemática o aleatoria en el sentido de que la primera información de estado es generada por el componente de control respectivo y una segunda información de estado separada es generada por el componente de monitorización respectivo, en donde el componente de monitorización y el componente de control están configurados para comparar la primera y la segunda información de estado intercambiadas entre sí o correspondientemente con información de estado predeterminada. Tanto el componente de monitorización como el componente de control están configurados para transferir el sistema de control al estado seguro si se reconoce una desviación de la primera y segunda información de estado entre sí o de la información de estado predeterminada en el componente de monitorización y/o en el componente de control, lo que indica un fallo.

De acuerdo con la invención, la primera información de estado contiene información sobre un estado (objetivo) del actuador detectado por el componente de control. En esta realización, la segunda información de estado es información sobre un estado (real) del actuador detectado por el componente de monitorización. De este modo, el componente de control y el componente de monitorización están configurados para detectar uno o más estados del actuador por separado y comparar esta información de estado entre sí y/o con información de estado predeterminada. Si esta información de estado difiere, esto es una indicación de que hay un fallo en el actuador y/o un fallo en uno de los componentes de control o en el componente de monitorización, que puede ser reconocido por el otro componente respectivo. Como se ha explicado con anterioridad, el componente de control y el componente de monitorización están configurados para transferir el sistema de control a un estado seguro en este caso.

De acuerdo con la invención, la primera información de estado contiene información sobre el estado del componente de control, mientras que la segunda información de estado es información sobre un estado del componente de monitor. En estas realizaciones, la primera y segunda información de estado son, por lo tanto, información sobre estados del componente de control y del componente de monitorización independiente de un estado del actuador. Así, según la invención, en estas realizaciones, la primera y segunda información de estado son información combinada sobre estados del componente de control y del componente de monitorización, así como sobre uno o más estados del actuador. En estas realizaciones del sistema de control, pueden detectarse, de este modo, errores que se producen independientemente de un estado del actuador (o de un error dentro del actuador), pero que se desencadenan puramente por un comportamiento defectuoso o un mal funcionamiento del componente de control o del componente de monitorización. También en estas realizaciones, el componente de control y el componente de monitorización se configuran en consecuencia para intercambiar la primera y segunda información de estado entre sí y para compararlas entre sí y/o con información de estado predeterminada, como se ha explicado con anterioridad. Por ejemplo, si la primera y la segunda información de estado comprenden información coincidente sobre un estado de funcionamiento normal del componente de monitorización y del componente de control, la primera y la segunda información de estado coinciden. Sin embargo, si uno de los

elementos de información de estado primero y segundo contiene, por ejemplo, información sobre un estado de desviación del componente de control o del componente de monitorización, los elementos de información de estado primero y segundo se desvían entre sí, lo que es reconocible en el otro componente. En tal caso, el otro componente se configura para transferir el sistema de control al estado seguro.

En diversas realizaciones, el componente de control y/o el componente de monitorización están configurados como microprocesadores de bajo coste que disponen de una conexión de red para enlazar con la red de comunicaciones y de las prestaciones correspondientes para implementar las funcionalidades requeridas. No tienen por qué ser componentes propietarios. En su lugar, el componente de control y el componente de monitorización se diseñan ventajosamente como componentes estándar de bajo coste que pueden utilizarse y configurarse de forma flexible y personalizada en el sistema de control.

En diversas realizaciones del sistema de control, este dispone de una fuente de alimentación central para suministrar energía eléctrica al sistema de control. Tanto el (al menos un) componente de monitorización como el (al menos un) componente de control están configurados para desconectar la fuente de alimentación central a fin de transferir el sistema de control al estado seguro. En estas realizaciones, el (al menos un) componente de monitorización y/o el (al menos un) componente de control están configurados de tal manera que la fuente de alimentación se desconecta si la comparación de la primera y segunda información de estado entre sí o correspondientemente con la información de estado predeterminada da como resultado una desviación de la primera y segunda información de estado entre sí o correspondientemente de la información de estado predeterminada. De este modo, el sistema de control puede transferirse al estado seguro desconectando la fuente de alimentación central. De este modo, el sistema de control puede desconectarse en forma segura en caso de avería, garantizando así que el estado seguro se mantiene de modo suficiente. Esto también ayuda a garantizar que el sistema de control está configurado con un alto nivel de integridad de seguridad.

En varias realizaciones del sistema de control, la red de comunicación se configura como una red inalámbrica. Esto tiene la ventaja de que los componentes del sistema de control, en particular el componente de control y/o el componente de monitorización, pueden configurarse como componentes distribuidos en ubicaciones distribuidas y separadas del sistema, por ejemplo, asignados a varios actuadores distribuidos del sistema de control. La red inalámbrica garantiza una red de comunicación flexible, personalizable y fácilmente escalable entre los respectivos componentes.

En diversas realizaciones del sistema de control, este comprende además al menos un componente de detección que está configurado para detectar un estado del actuador y transmitir información sobre el estado detectado al componente de monitorización. Esto significa que el componente de monitorización supervisa el estado del actuador utilizando la información del componente de detección sobre el estado detectado del actuador. En diversas realizaciones, el componente de detección es un sensor o un sistema de varios sensores. En otras realizaciones, varios componentes de detección se combinan para formar un sistema de detección. El componente de detección comprende, por ejemplo, fotodetectores para la monitorización (no reactiva) del estado de un actuador emisor de luz, una construcción de fibra óptica para la detección (no reactiva) de procesos de conmutación mecánica en un actuador mediante la detección de vibraciones (la denominada detección por fibra óptica) o un manguito inductivo para la detección (no reactiva) de corrientes eléctricas en o sobre un actuador.

En al menos una realización, el sistema de control comprende, además, al menos un componente de detección que está configurado para detectar un estado del actuador y transmitir información sobre el estado detectado al componente de control. En estas implementaciones, el componente de control detecta un estado del actuador utilizando la información del componente de detección sobre el estado detectado del actuador. El componente de control está configurado de tal manera que detecta información sobre el estado del actuador y la utiliza para controlar el actuador (por ejemplo, mediante señales de control del componente de control en la dirección del actuador).

En al menos una realización del sistema de control, el componente de monitorización está configurado para monitorizar el estado del actuador sin realimentación y/o independientemente del componente de control. Monitorización sin retroalimentación significa aquí que la monitorización del estado del actuador por el componente de monitorización no tiene efecto en el estado del actuador (y posiblemente tampoco en los estados de otros componentes dentro del sistema de control o en la red de comunicación). La monitorización independiente del componente de control por parte del componente de monitorización significa que la retroalimentación sobre uno o más estados del actuador se recibe a través del componente de monitorización, que tiene lugar a través de un canal diferente y separado de la retroalimentación entre el actuador y el componente de control. Por lo tanto, esta realización tiene la ventaja de que, a pesar de los componentes sencillos y económicos, se puede realizar de manera sencilla un sistema de control multicanal en el sentido de un concepto de seguridad del tipo explicado con anterioridad. De este modo, la monitorización del estado del actuador a través del componente de monitorización tiene lugar por separado de cualquier monitorización del estado del actuador a través del componente de control. De este modo, la primera información de estado se genera en forma separada e independiente de la segunda información de estado, con lo que se realizan dos canales separados para detectar posibles fallos en el actuador, en el componente de control o en el componente de monitorización.

En varias realizaciones del sistema de control, una o más informaciones de estado predeterminadas sobre estados definidos del actuador y/o del componente de control y/o del componente de monitorización se almacenan en la red de comunicación. En al menos una realización, esta información de estado predeterminada corresponde a la información de estado predeterminada del tipo explicado con anterioridad. El componente de control y/o el componente de monitorización están configurados para comparar la primera y/o segunda información de estado con la información de estado predeterminada. Además, tanto el componente de monitorización como el componente de control están configurados para transferir el sistema de control al estado seguro si una comparación de la primera y/o segunda información de estado con la información de estado predeterminada revela una desviación de la primera y/o segunda información de estado de la información de estado predeterminada. En estas realizaciones, la información de estado predeterminada (información de referencia) se almacena en la red de comunicación, por ejemplo, en forma de una o más listas o tablas. En realizaciones especiales, la información de estado se almacena en el componente de control o en el propio componente de monitorización. En realizaciones alternativas, la información de estado predeterminada se almacena en uno o más componentes separados del sistema de control, que también están integrados en la red de comunicación y pueden intercambiar información con el componente de control y/o con el componente de monitorización.

La información de estado predeterminada comprende ventajosamente información sobre estados definidos, es decir, predeterminados (correctos) del actuador y/o del componente de control y/o del componente de monitorización. Esto tiene la ventaja de que, al comparar la primera y/o la segunda información de estado con la información de estado predeterminada, se puede reconocer un error en el actuador, en el componente de control o en el componente de monitorización, incluso si este error influye en la primera y la segunda información de estado de tal manera que coincidan y no se desvíen entre sí. Esto ocurre, por ejemplo, en el caso de un error acumulativo tanto en el componente de control como en el componente de monitorización o en el caso de un error en el actuador que hace coincidir la primera y la segunda información de estado. No obstante, el sistema de control también está implementado para tales situaciones, como se ha explicado con anterioridad, en las que la primera y/o segunda información de estado es comparable con la información de estado predeterminada, de modo que puede reconocerse una desviación de los estados detectados dentro del sistema de control con respecto a los estados predefinidos (mediante la información de estado predeterminada). En caso de que se produzca tal desviación, el sistema de control se configura en consecuencia para ser transferido al estado seguro por medio del componente de control y/o por medio del componente de monitorización.

Esto también es ventajoso en las realizaciones del sistema de control en las que se ha configurado una pluralidad de componentes de control y/o una pluralidad de componentes de monitorización, ya que un fallo de uno o más componentes de control acumulado con uno o más componentes de monitorización (que puede conducir a la coincidencia de la primera y segunda información de estado) puede ser reconocido por otros componentes de control o monitorización. En este caso, todos los componentes de control o de monitorización están configurados para intercambiar primera y segunda información de estado entre sí a través de la red de comunicación y para compararla con la información de estado predeterminada, de modo que puedan reconocerse las desviaciones o los fallos. Esto aumenta aún más la seguridad del sistema de control.

En al menos una realización del sistema de control, la red de comunicación se configura utilizando un protocolo de red tolerante a fallos. El componente de control y el componente de monitorización están configurados para comunicarse a través del protocolo de red tolerante a fallos de la red de comunicación. De este modo, el sistema de control está protegido contra errores malintencionados o arbitrarios por parte de uno de los participantes de la red (componentes) dentro de la red de comunicación. Incluso si, por ejemplo, un componente de control o un componente de monitorización intercambia información divergente con varios otros componentes del sistema de control, o si, por ejemplo, la información de estado predeterminada almacenada del tipo explicado con anterioridad diverge debido a un error (por ejemplo, listas desviadas o falsificadas de estados definidos), el sistema de control sigue siendo robusto contra tales escenarios debido al protocolo de red tolerante a fallos. En una realización, el protocolo de red tolerante a fallos es, por ejemplo, un protocolo según la denominada tolerancia a fallos bizantina (BFT). Esto tiene la ventaja, en particular en las implementaciones del sistema de control con un mayor número de componentes de control o monitorización, de que cualquier comportamiento incorrecto de una minoría de los componentes, por ejemplo, una falsificación de la información de estado predeterminada del tipo explicado con anterioridad, todavía se puede detectar y procesar de forma fiable dentro del sistema de control, de modo que el sistema de control se puede transferir al estado seguro de una manera ordenada.

En al menos una realización del sistema de control, se configura una denominada infraestructura de clave pública (PKI) para el componente de control y para el componente de guardia. Esto tiene la ventaja de que se garantiza una identificación única de los componentes implicados mediante certificados digitales. Esto también sirve a aspectos de seguridad, ya que facilita la revelación y detección de errores.

En al menos una realización del sistema de control, uno o más módulos GPS están configurados para apoyar la sincronización horaria entre los componentes implicados. Esto tiene la ventaja de que la sincronización entre los componentes implicados puede llevarse a cabo en forma fiable.

En al menos una realización del sistema de control, el componente de control y el componente de monitorización

están configurados para realizar un procesamiento cíclico, en particular de la primera y segunda información de estado. Por ejemplo, en cada ciclo, el componente de control y/o el componente de monitorización leen la información procedente del actuador (posiblemente a través de uno o varios componentes de detección o componentes de entrada externos descritos con anterioridad), se procesa/comunica/sincroniza en o entre el componente de control y el componente de monitorización a través de la red de comunicación y, si es necesario, se emiten órdenes, comandos, etc., en particular al actuador y/o se transfiere el sistema de control al estado seguro. El procesamiento cíclico tiene la ventaja de que se pueden utilizar componentes más sencillos que funcionen según un esquema de procesamiento cíclico. Además, se puede conseguir una garantía de tiempo en la que el siguiente cambio de estado dentro de la red de comunicación (estados sincronizados del actuador, el componente de control y el componente de monitorización u otros componentes) tenga lugar en momentos fijos. Esto tiene la ventaja de que se garantiza una reacción definida del sistema de control una vez completado un ciclo. De este modo, los fallos pueden reconocerse de manera rápida y, a la vez, sencilla.

En realizaciones alternativas, se lleva a cabo el procesamiento no cíclico de estados o información de estado. Aquí, por ejemplo, la información de estado activada por eventos se transmite desde un componente (componente de control o componente de monitorización) a otro componente correspondiente dentro de la red de comunicación, que activa el procesamiento de la información. El procesamiento no cíclico tiene la ventaja de una gran flexibilidad y una respuesta muy rápida a los errores.

En diversas realizaciones del sistema de control, se trata de un sistema de señalización/interbloqueo para vehículos ferroviarios.

La tarea anterior se resuelve según un segundo aspecto mediante un procedimiento de acuerdo con la reivindicación de patente 9, que se implementa para operar un sistema de control. Otras implementaciones se describen en las subreivindicaciones asociadas.

Dicho procedimiento se implementa para operar un sistema de control que tiene al menos un actuador, al menos un componente de control, al menos un componente de monitorización y una red de comunicación. El componente de control controla el actuador, mientras que el componente de monitorización supervisa el estado del actuador. El procedimiento comprende los siguientes pasos:

- generación de una primera información de estado por el componente de control,

- generación de una segunda información de estado por el componente de monitorización,

- intercambio de la primera y segunda información de estado entre el componente de control y el componente de monitorización a través de la red de comunicación,

- comparación de la primera y segunda información de estado (intercambiada) entre sí y/o correspondientemente con información de estado predeterminada por el componente de control y por el componente de monitorización, y

- transferencia del sistema de control a un estado seguro por el componente de control y/o por el componente de monitorización si la comparación de la primera y segunda información de estado entre sí y/o correspondientemente con la información de estado predeterminada da como resultado una desviación de la primera y segunda información de estado entre sí y/o correspondientemente de la información de estado predeterminada.

Este procedimiento tiene la ventaja de que, en lugar de una unidad de cálculo central y compleja, se utilizan componentes sencillos (componente de control y componente de monitorización), que son baratos y, aun así, proporcionan un nivel de seguridad suficientemente alto para las funciones del sistema de control. De este modo, el sistema de control puede implementarse en forma rentable y funcionar con un nivel de seguridad muy elevado. Por lo demás, con este procedimiento también se consiguen ventajas y efectos como los explicados con anterioridad en relación con un sistema de control.

En al menos una realización del procedimiento, el sistema de control comprende una fuente de alimentación central para suministrar energía eléctrica al sistema de control, en donde el sistema de control se transfiere al estado seguro mediante la desconexión de la fuente de alimentación central por el (al menos un) componente de control y/o por el (al menos un) componente de monitorización. De este modo, el procedimiento tiene la ventaja de que la desconexión de la fuente de alimentación central permite un mantenimiento suficiente del estado seguro. Además, las ventajas y los efectos explicados con anterioridad en relación con un sistema de control correspondiente se aplican aquí de manera análoga.

En al menos una realización del procedimiento, el sistema de control comprende un componente de detección, en el que el componente de detección detecta un estado del actuador y transmite información sobre el estado detectado al componente de monitorización. De este modo, el estado del actuador se detecta en forma sencilla y se transmite al componente de monitorización. Además, las ventajas y efectos explicados con anterioridad en relación con un sistema fiscal se aplican de manera análoga en este caso.

En al menos una realización del procedimiento, el componente de monitorización supervisa el estado del actuador sin realimentación y/o independientemente del componente de control. De este modo, las ventajas y los efectos explicados con anterioridad en relación con un sistema de control se consiguen de manera análoga.

En al menos una realización del procedimiento, se almacena en la red de comunicación información de estado predeterminada sobre estados definidos del actuador y/o del componente de control y/o del componente de monitorización. En al menos una realización del procedimiento, esta información de estado predeterminada corresponde a la información de estado predeterminada del tipo explicado con anterioridad. El procedimiento se implementa de tal manera que

- la primera y/o segunda información de estado se compara con la información de estado predeterminada por el componente de control y/o por el componente de monitorización y

- el sistema de control se transfiere a un estado seguro por el componente de control y/o por el componente de monitorización si la comparación de la primera y/o segunda información de estado con la información de estado predeterminada da como resultado una desviación de la primera y/o segunda información de estado de la información de estado predeterminada. Las ventajas y efectos explicados con anterioridad en relación con el sistema de control se consiguen de forma análoga mediante el procedimiento.

En al menos una realización del procedimiento, la red de comunicación se establece utilizando un protocolo de red tolerante a fallos, comunicándose el componente de control y el componente de monitorización a través del protocolo de red tolerante a fallos de la red de comunicación. De este modo, el procedimiento consigue las ventajas y los efectos explicados con anterioridad en relación con un sistema de control por analogía.

El sistema de control según el primer aspecto está ventajosamente dispuesto para realizar un procedimiento según el segundo aspecto.

La tarea anterior se resuelve según un tercer aspecto mediante un programa de control de acuerdo con la reivindicación de patente 15. El programa de control está configurado para ejecutarse dentro de un sistema de control y, cuando se ejecuta dentro del sistema de control, para llevar a cabo un procedimiento del tipo explicado con anterioridad. En este caso, el sistema de control se implementa, por ejemplo, de la manera descrita con anterioridad.

Todas las características, implementaciones, aspectos, ventajas y efectos de un sistema de control según el primer aspecto son transferibles a las características, implementaciones, aspectos, ventajas y efectos correspondientes de un procedimiento según el segundo aspecto, y viceversa.

Las anteriores propiedades, características y ventajas de la invención y la forma en que se consiguen se explican con más detalle en la siguiente descripción de las realizaciones de la invención junto con las Figuras correspondientes.

En este caso:

Figura 1 muestra un primer ejemplo de realización de un sistema de control,

Figura 2 muestra un segundo ejemplo de realización de un sistema de control,

Figura 3 muestra un primer ejemplo de implementación de un procedimiento para operar un sistema de control y

Figura 4 muestra un segundo ejemplo de implementación de un procedimiento para operar un sistema de control.

La Figura 1 muestra un sistema 1 de control con varios actuadores 2a a 2d, varios componentes 4a a 4d de control y varios componentes 5a a 5d de monitorización. Los componentes 4a a 4d de control y los componentes 5a a 5d de monitorización están conectados a una red 3 de comunicación y están configurados para comunicarse entre sí en la red 3 de comunicación. Un componente 4a a 4d de control respectivo se asigna a un actuador 2a a 2d respectivo y se configura para controlar el actuador 2a a 2d respectivo. En concreto, el componente 4a de control se asigna al actuador 2a, el componente 4b de control se asigna al actuador 2b, el componente 4c de control se asigna al actuador 2c y el componente 4d de control se asigna al actuador 2d. En una realización alternativa, todos los componentes 4a a 4d de control están interconectados a través de la red 3 de comunicación, por lo que un componente de control puede controlar cualquiera de los actuadores 2a a 2d.

En el ejemplo de realización mostrado en la Figura 1, los respectivos componentes 4a a 4d de control intercambian información, datos o señales con los respectivos actuadores 2a a 2d. Esto se ilustra, en cada caso, mediante una flecha bidireccional entre el respectivo componente 4a a 4d de control y el respectivo actuador 2a a 2d. Por ejemplo, un componente 4a a 4d de control respectivo envía una señal de control a un actuador 2a a 2d respectivo para controlar el actuador 2a a 2d. Opcionalmente, un componente 4a a 4d de control respectivo también detecta uno o más estados del respectivo actuador 2a a 2d asociado. Por ejemplo, un componente 4a a 4d de control respectivo

especifica cierto estado objetivo de un actuador 2a a 2d asociado, por lo que el actuador 2a a 2d respectivo se controla en consecuencia. Opcionalmente, un estado real correspondiente del actuador 2a a 2d se devuelve al componente 4a a 4d de control respectivo.

En el ejemplo de realización según la Figura 1, un componente 5a a 5d de monitorización respectivo está conectado a uno de varios componentes 8a a 8d de detección. En concreto, según la Figura 1, el componente 5a de monitorización está conectado al componente 8a de detección, el componente 5b de monitorización está conectado al componente 8b de detección, el componente 5c de monitorización está conectado al componente 8c de detección y el componente 5d de monitorización está conectado al componente 8d de detección. Los respectivos componentes 8a a 8d de detección están, a su vez, asignados a un respectivo actuador 2a a 2d. En concreto, el componente 8a de detección se asigna al actuador 2a, el componente 8b de detección al actuador 2b, el componente 8c de detección al actuador 2c y el componente 8d de detección al actuador 2d. Los respectivos componentes 8a a 8d de detección están configurados para detectar uno o más estados del respectivo actuador 2a a 2d y para transferir información sobre el estado detectado al respectivo componente 5a a 5d de monitorización. De este modo, un componente 5a a 5d de monitorización respectivo monitoriza un estado respectivo del actuador 2a a 2d respectivo por separado e independientemente de un intercambio respectivo de información entre un actuador 2a a 2d respectivo y un componente 4a a 4d de control asociado respectivo. De este modo, se establecen canales separados para detectar información entre los respectivos actuadores 2a a 2d y los respectivos componentes 4a a 4d de control y los respectivos actuadores 2a a 2d mediante los respectivos componentes 8a a 8d de detección y los respectivos componentes 5a a 5d de monitorización.

Los respectivos componentes 8a a 8d de detección son, por ejemplo, un sensor para la detección no reactiva de un estado respectivo del respectivo actuador 2a a 2d. Los componentes 8a a 8d de detección incluyen, por ejemplo, fotodetectores para la monitorización no reactiva del estado de un actuador 2a a 2d emisor de luz, una construcción de fibra óptica para la detección no reactiva de procesos de conmutación mecánica en un actuador 2a a 2d respectivo mediante la detección de vibraciones (la denominada detección de fibra óptica) o un manguito inductivo para la detección no reactiva de corrientes eléctricas en o sobre un actuador 2a a 2d respectivo. Los componentes 4a a 4d de control o los componentes 5a a 5d de monitorización son microprocesadores económicos con una conexión de red a la red 3 de comunicación en el ejemplo de diseño mostrado en la Figura 1.

De acuerdo con el ejemplo de realización de la Figura 1, el sistema 1 de control también dispone de un sensor 6 externo y una fuente 7 de alimentación central para suministrar energía eléctrica al sistema de control. El sensor 6 externo está configurado para detectar otras señales o informaciones de entrada externas. El sensor 6 externo está integrado en la red 3 de comunicación de manera que intercambia la información correspondiente con los demás componentes del sistema 1 de control. La fuente 7 de alimentación central está conectada a la red 3 de comunicación de tal manera que la fuente 7 de alimentación central puede desconectarse a través de uno de los componentes 4a a 4d de control o uno de los componentes 5a a 5d de monitorización. De este modo, el sistema 1 de control puede desconectarse a través de cada uno de los componentes 4a a 4d de control y cada uno de los componentes 5a a 5d de monitorización. La desconexión del sistema 1 de control lo pone en un estado seguro.

El sistema 1 de control según el ejemplo de diseño de la Figura 1 se implementa de tal manera que se consigue un alto grado de seguridad mediante una pluralidad de componentes 4a a 4d y 5a a 5d distribuidos. A pesar del diseño simple de todos los componentes 4a a 4d y 5a a 5d, se garantiza la capacidad multicanal en la monitorización, activación o desactivación de los actuadores 2a a 2d individuales o del propio sistema 1 de control. Además, la capacidad de desconectar el sistema 1 de control a través de la fuente 7 de alimentación central garantiza que el sistema 1 de control pueda transferirse en forma segura a un estado seguro (estado desconectado) y que este estado seguro pueda mantenerse. De este modo, el sistema 1 de control cumple un nivel muy alto de integridad de la seguridad a pesar de su implementación sencilla y rentable. La activación, monitorización y desconexión dentro del sistema 1 de control se realiza a través de los componentes 4a a 4d y 5a a 5d distribuidos, que comparten dichas tareas y proporcionan una monitorización multicanal.

En el ejemplo de realización mostrado en la Figura 1, los componentes 4a a 4d y 5a a 5d se comunican dentro de la red 3 de comunicación mediante un protocolo de red tolerante a fallos, en particular un protocolo de red que se implementa de acuerdo con la denominada tolerancia a fallos bizantina (BFT). El protocolo de red de la red 3 de comunicación también permite una sincronización rápida y segura de todos los componentes 4a a 4d y 5a a 5d para intercambiar información entre sí, como se explicará con más detalle a continuación. Para identificar de manera inequívoca los componentes 4a a 4d y 5a a 5d (y posiblemente otros componentes), estos están conectados a través de una infraestructura PKI, por ejemplo, mediante la cual pueden intercambiarse certificados entre los componentes. Esto también sirve a aspectos de seguridad porque facilita la revelación de errores. Opcionalmente, la red 3 de comunicación dispone de módulos GPS que permiten la sincronización horaria.

Los respectivos componentes 4a a 4d de control generan cada uno una primera información de estado que representa un estado del respectivo actuador 2a a 2d y/o un respectivo estado del componente 4a a 4d de control. Los respectivos componentes 5a a 5d de monitorización generan una segunda información de estado, que representa información de los respectivos componentes 8a a 8d de detección sobre un estado de los respectivos actuadores 2a a 2d y/o un estado respectivo de los propios componentes 5a a 5d de monitorización. La primera y

la segunda información de estado se intercambian entre los componentes conectados 4a a 4d y 5a a 5d en la red 3 de comunicación inteligente. Esto tiene lugar, por ejemplo, como parte de una sincronización de todos los componentes 4a a 4d y 5a a 5d dentro de la red 3 de comunicación. En los respectivos componentes 4a a 4d y 5a a 5d, la primera y segunda información de estado se comparan entre sí y/o con información de estado predeterminada almacenada allí. La información de estado predeterminada incluye, por ejemplo, información sobre estados predefinidos de los actuadores 2a a 2d, los componentes 4a a 4d de control y/o los componentes 5a a 5d de monitorización (y posiblemente otros componentes).

Comparando la primera y la segunda información de estado entre sí o con la información de estado predeterminada dentro de los respectivos componentes 4a a 4d y 5a a 5d, se determina si la información de estado respectiva se desvía o coincide entre sí. En el caso de que se detecte una desviación entre la información de estado respectiva en al menos uno de los componentes 4a a 4d y 5a a 5d (o a través de un componente de procesamiento de nivel superior dentro de la red 3 de comunicación), se infiere un fallo dentro del sistema 1 de control. En este caso, al menos uno de los componentes 4a a 4d y 5a a 5d desconecta la fuente 7 de alimentación central del sistema 1 de control para que pase a un estado sin tensión (seguro).

Un error correspondiente puede ser, por ejemplo, una discrepancia entre un estado objetivo y un estado real de un actuador 2a a 2d respectivo, en donde un estado objetivo se genera como primera información de estado en un componente 4a a 4d de control respectivo y un estado real es detectado por un componente 8a a 8d de detección respectivo y se genera dentro de un componente 5a a 5d de monitorización respectivo como segunda información de estado. Mediante la sincronización dentro de la red 3 de comunicación y la comparación de la primera y segunda información de estado, se detecta consecuentemente tal discrepancia entre el estado objetivo y el estado real de un actuador 2a a 2d.

Alternativa o adicionalmente, determinados estados de los componentes 4a a 4d de control o de los propios componentes 5a a 5d de monitorización conducen a la correspondiente primera y segunda información de estado. Esto incluye, por ejemplo, información sobre el funcionamiento normal o el funcionamiento defectuoso/fallo de los respectivos componentes 4a a 4d y 5a a 5d. Si la comparación de la primera y la segunda información de estado da como resultado una discrepancia en este caso (por ejemplo, entre el funcionamiento normal y el funcionamiento defectuoso), se detecta también un comportamiento defectuoso del sistema 1 de control.

Alternativa o adicionalmente, la primera y segunda información de estado se compara con la información de estado predeterminada explicada con anterioridad. Si la primera y/o segunda información de estado se desvía de la información de estado predeterminada, también se deduce un fallo. Este procedimiento tiene la ventaja de que los fallos se reconocen incluso si no hay desviación entre la primera y segunda información de estado, pero hay una desviación entre la primera y/o segunda información de estado y la información de estado predeterminada. Esto ocurre, por ejemplo, si se produce un fallo aleatorio o sistemático en uno de los actuadores 2a a 2d, lo que provoca una coincidencia entre la primera y la segunda información de estado en los componentes 4a a 4d o 5a a 5d. La comparación con la información de estado predeterminada lleva a reconocer un estado indefinido del actuador 2a a 2d defectuoso. Lo mismo se aplica en el caso de que se produzca un fallo acumulativo, por ejemplo, en el componente 4a de control y en el componente 5a de monitorización (por ejemplo, un fallo de ambos componentes 4a y 5a), lo que también puede dar lugar a que coincidan la primera y la segunda información de estado. No obstante, se reconoce una desviación de esta primera y segunda información de estado con respecto a la información de estado predeterminada de un estado definido (por ejemplo, el funcionamiento normal de los componentes 4a y 5a).

Si se produce uno de los fallos descritos con anterioridad en el sistema 1 de control, cada uno de los componentes 4a a 4d y 5a a 5d puede desconectar la fuente 7 de alimentación central y transferir el sistema 1 de control al estado seguro descrito con anterioridad. Esto tiene la ventaja de que el sistema 1 de control tiene un alto grado de seguridad contra fallos individuales, pero también seguridad en caso de fallos acumulativos. En particular, el sistema 1 de control reacciona así favorablemente ante errores aleatorios (por ejemplo, fallo físico de uno o varios componentes del sistema 1 de control) o ante errores sistemáticos (por ejemplo, errores en la programación o programación incorrecta de uno o varios componentes del sistema 1 de control). Por lo tanto, el sistema 1 de control es ventajosamente apto para SIL2 o SIL3.

La Figura 2 muestra un segundo ejemplo de realización de un sistema 1 de control. Los componentes etiquetados con los mismos símbolos de referencia corresponden a los componentes y sus funciones tal como se explican para el ejemplo de realización del sistema 1 de control según la Figura 1.

En contraste con el ejemplo de realización según la Figura 1, el ejemplo de realización del sistema 1 de control según la Figura 2 presenta solo dos componentes 5a y 5b de monitorización, que están conectados cada uno a un sistema 9a y 9b de detección, respectivamente. Los dos sistemas 9a y 9b de detección comprenden cada uno dos componentes 8a y 8b y 8c y 8d de detección, respectivamente, que están conectados a los correspondientes actuadores 2a a 2d de la misma manera que en el ejemplo de realización mostrado en la Figura 1 con el fin de detectar sus estados.

En el ejemplo de realización mostrado en la Figura 2, los actuadores 2a a 2d comprenden cada uno una pluralidad de dispositivos 10a a 10c de señalización, que son, por ejemplo, iluminantes de un sistema de señalización. Por ejemplo, los actuadores 2a y 2b se utilizan para la señalización de un vehículo ferroviario en un primer sentido de la marcha, mientras que los actuadores 2c y 2d se utilizan para la señalización de un vehículo ferroviario en un segundo sentido de la marcha. Por ejemplo, existen tres configuraciones luminosas diferentes 10a a 10c para cada actuador 2a a 2d, en cada una de las cuales se enciende un dispositivo 10a a 10c de señalización y se apagan los demás dispositivos 10a a 10c de señalización.

El sensor 6 externo en el ejemplo de realización según la Figura 2 es, por ejemplo, un sensor de aproximación para vehículos de carretera como entrada externa del sistema 1 de control. El sistema 1 de control según la Figura 2 es, por ejemplo, un sistema de señalización/posicionamiento para vehículos ferroviarios.

Los respectivos componentes 4a a 4d de control pueden controlar los respectivos actuadores 2a a 2d asignados y sus configuraciones 10a a 10c luminosas en función de una entrada procedente del sensor 6 externo. Los estados de iluminación de los respectivos actuadores 2a a 2d se detectan a través de los correspondientes componentes 8a a 8d de detección y se transmiten a los respectivos componentes 5a y 5b de monitorización. De este modo, los estados de consigna de los respectivos actuadores 2a a 2d se procesan y registran en los componentes 4a a 4d de control y los estados reales de los respectivos actuadores 2a a 2d se procesan y registran en los componentes 5a y 5b de monitorización. Estos estados teóricos y reales se registran, procesan y sincronizan cíclicamente por los componentes implicados dentro de la red 3 de comunicación. A continuación, los estados teórico y real se comparan entre sí en los componentes 4a a 4d o 5a y 5b participantes y se detectan desviaciones o errores. En este caso, uno de los componentes 4a a 4d o 5a y 5b desconecta el sistema 1 de control mediante la orden correspondiente al final de un ciclo de procesamiento a través de la fuente 7 de alimentación eléctrica.

Alternativa o adicionalmente, las configuraciones 10a a 10c luminosas autorizadas para cada uno de los actuadores 2a a 2d se almacenan en la red 3 de comunicación, por ejemplo, dentro de los componentes 4a a 4d y 5a y 5b en forma de listas. De este modo, se detectan estados desviados de los actuadores 2a a 2d (debido a un error), por ejemplo, una señalización “verde” de todos los actuadores 2a a 2d participantes, como se ha explicado en general para el ejemplo de realización según la Figura 1 anterior, por lo que cada uno de los componentes 4a a 4d y 5a o 5b puede desconectar el sistema 1 de control de acuerdo con las explicaciones anteriores. De este modo, se detectan posibles errores sistemáticos (por ejemplo, un error complejo en una representación de diodos multicolor dentro de los actuadores 2a a 2d), ya que estos darían lugar a que se produjeran configuraciones de iluminación no permitidas, que se detectan comparando la primera y la segunda información de estado correspondiente con la información de estado predeterminada almacenada.

Un estado peligroso del sistema 1 de control en el ejemplo de realización según la Figura 2 está dado, por ejemplo, por el hecho de que, para al menos un actuador 2a y 2b y al menos un actuador 2c y 2d (para diferentes sentidos de marcha, como se ha explicado con anterioridad), existe una señal verde, por ejemplo, 10a durante al menos un ciclo de procesamiento dentro de la red 3 de comunicación. Este estado peligroso puede alcanzarse, por ejemplo, si se produce un tipo de error sistemático extremadamente complejo en forma coordinada y alterna periódicamente en todos los componentes 4a a 4d de control, en los componentes 5a y 5b de monitorización y en los componentes 8a a 8d de detección, de modo que ninguno de los componentes conectados a la red 3 de comunicación reconozca la desviación de la información de estado predeterminada almacenada (estados definidos/permitidos o configuraciones 10a a 10c luminosas) y garantice la desconexión inmediata del sistema 1 de control. Gracias al procesamiento cíclico del proceso descrito con anterioridad, los errores sistemáticos de este tipo pueden descartarse eficazmente.

Otras causas aleatorias de peligro son, por ejemplo, un fallo físico de uno o más componentes del sistema 1 de control. Debido a la comparación de la primera y la segunda información de estado entre sí o con información de estado predeterminada, como se ha explicado con anterioridad, cada uno de los componentes 4a a 4d o 5a y 5b puede detectar una desviación al final de un ciclo a más tardar mediante la sincronización cíclica dentro de la red 3 de comunicación, de modo que se detecta un fallo en el sistema 1 de control después de un ciclo a más tardar y se activa una desconexión.

De este modo, incluso un fallo de los componentes 4a y 4b de control, así como del componente 5a de monitorización es detectado por al menos uno de los otros componentes 4c y 4d o 5b mediante sincronización cíclica dentro de la red 3 de comunicación si los estados de los componentes 4a, 4b y 5a averiados se desvían de los estados predeterminados. Los fallos aleatorios de los actuadores 2a a 2d también se reconocen después de un ciclo como máximo. Los fallos aleatorios del sensor 6 de accionamiento solo son relevantes para la disponibilidad. Los fallos aleatorios al desconectar la fuente 7 de alimentación central se controlan ventajosamente mediante un diseño multicanal.

La Figura 3 muestra un primer ejemplo de implementación de un procedimiento para operar un sistema 1 de control. Dicho sistema de control se construye, por ejemplo, de acuerdo con una de las realizaciones mostradas en las Figuras 1 y 2. En un paso S1, se genera G una primera pieza de información de estado Z1, por ejemplo, por un componente 4a a 4d de control del tipo descrito con anterioridad. En un paso S2, se genera G una segunda

información de estado Z2, por ejemplo, por un componente 5a a 5d de monitorización del tipo descrito con anterioridad. En otro paso S3, la primera y segunda información de estado Z1 y Z2 se intercambian o sincronizan S, por ejemplo, entre todos los componentes 4a a 4d de control y todos los componentes 5a a 5d de monitorización a través de la red 3 de comunicación, como se ha explicado con anterioridad. En un paso S4, se lleva a cabo una comparación E de la primera y segunda información de estado Z1 y Z2 intercambiadas, por ejemplo, por los componentes 4a a 4d de control y/o por los componentes 5a a 5d de monitorización, como se ha explicado con anterioridad. Finalmente, en un paso S5, el sistema 1 de control se transfiere C a un estado seguro, por ejemplo, por uno de los componentes 4a a 4d de control y/o por uno de los componentes 5a a 5d de monitorización, como se ha explicado con anterioridad, si la comparación E de la primera y segunda información de estado Z1 y Z2 en el paso S4 da como resultado una desviación de la primera y segunda información de estado Z1 y Z2 entre sí.

La Figura 4 muestra un segundo ejemplo de realización de un procedimiento para hacer funcionar un sistema 1 de control, que se construye, por ejemplo, según una de las realizaciones de las Figuras 1 y 2. El ejemplo de realización según la Figura 4 comprende los pasos del procedimiento tal como se explican para la Figura 3. Alternativamente o además de un paso S4 según la Figura 3, la realización según la Figura 4 comprende un paso adicional S5, en el que se lleva a cabo una comparación adicional E de la primera y/o segunda información de estado Z1 y Z2 con la información de estado predeterminada Zdef, por ejemplo, por uno de los componentes 4a a 4d de control y/o por uno de los componentes 5a a 5d de monitorización, como se ha explicado con anterioridad. La información de estado predeterminada Zdef es, por ejemplo, dicha información de estado predeterminada como se ha explicado con anterioridad en relación con los ejemplos de realización según las Figuras 1 y 2.

Además, en un paso S6 en el ejemplo de realización según la Figura 4, el sistema 1 de control se transfiere C al estado seguro, por ejemplo, por un componente 4a a 4d de control y/o por un componente 5a a 5d de monitorización, como se ha explicado con anterioridad, si la comparación E en el paso S4 y/o la comparación E en el paso S5 ha mostrado que la primera y/o la segunda información de estado Z1 y Z2 se desvían entre sí o de la información de estado predeterminada Zdef.

Los ejemplos de diseño e implementación mostrados son meros ejemplos. Pueden preverse diferentes variantes. Por ejemplo, la red 3 de comunicación en los ejemplos de realización de las Figuras 1 y 2 está configurada como una red cableada o como una red inalámbrica. En una realización alternativa al ejemplo de realización mostrado en la Figura 2, pueden configurarse más de dos componentes 5a y 5b de monitorización, en particular, por ejemplo, cuatro componentes 5a a 5d de monitorización, en forma análoga al ejemplo de realización mostrado en la Figura 1, cada uno de los cuales está asignado a un componente 8a a 8d de detección. Un sistema 1 de control es, por ejemplo, un sistema de señalización/enclavamiento para vehículos ferroviarios, en particular vehículos ferroviarios eléctricos, o alternativamente un sistema de señalización en el tráfico por carretera. Alternativamente, el sistema 1 de control es un sistema de control dentro de una planta industrial o dentro de un sistema de automatización de edificios.

Aunque la invención se ha ilustrado y descrito en detalle mediante ejemplos de realización, la invención no se limita a los ejemplos de realización divulgados y a las combinaciones específicas de características explicadas en los mismos. Un experto en la técnica puede obtener otras variaciones de la invención sin apartarse del ámbito de protección de la invención reivindicada.

Lista de signos de referencia

1	Sistema de control
2a a 2d	Actuador
3	Red de comunicación
4a a 4d	Componente de control
5a a 5d	Componente de monitorización
6	Sensor externo
7	Fuente de alimentación central
8a a 8d	Componente de detección
9a, 9b	Sistema de detección
10a a 10c	Dispositivo de señalización/configuración luminosa
Z1	Primera información de estado

Z2	Segunda información de estado
Zdef	Información de estado predeterminada
G	Generación
S	Intercambio
E	Comparación
C	Transferencia
S1 a S6	Pasos del procedimiento

REIVINDICACIONES

1. Sistema (1) de control con:

- al menos un actuador (2a, ..., 2d),

- una pluralidad m de componentes (4a, ..., 4d) de control, que están configurados para controlar el al menos un actuador (2a, ..., 2d) y generar al menos una primera información de estado (Z1),

- una pluralidad n de componentes (5a, ..., 5d) de monitorización, que están configurados para supervisar un estado del al menos un actuador (2a, ..., 2d) y generar al menos una segunda información de estado (Z2), y

- una red (3) de comunicación, en donde una o más informaciones de estado (Zdef) predeterminadas sobre estados definidos del actuador (2a, ..., 2d) y/o el componente de control y/o el componente de monitorización se almacenan en la red de comunicación,

- una fuente (7) de alimentación central para suministrar energía eléctrica al sistema (1) de control,

en donde los componentes (5a, ..., 5d) de monitorización y los componentes (4a, ..., 4d) de control

- se integran en la red (3) de comunicación, y

- están configurados para intercambiar entre sí la primera y la segunda información de estado (Z1, Z2) a través de la red (3) de comunicación, y

- están configurados para comparar la primera y la segunda información de estado (Z1, Z2) entre sí y/o de acuerdo con la información de estado predeterminada (Zdef), y

- están configurados para desconectar la fuente (7) de alimentación central con el fin de transferir el sistema (1) de control a un estado seguro si una comparación de la primera y segunda información de estado (Z1, Z2) entre sí y/o correspondientemente con la información de estado predeterminada (Zdef), resulta una desviación de la primera y segunda información de estado (Z1, Z2) entre sí y/o correspondientemente de la información de estado predeterminada (Zdef),

en donde

- la primera y segunda información de estado (Z1, Z2) es información combinada sobre los estados del componente (4a, ..., 4d) de control y del componente (5a, ..., 5d) de monitorización y sobre uno o más estados del actuador (2a, ..., 2d), y

- la primera información de estado (Z1) contiene información sobre un estado del actuador (2a, ..., 2d) detectado por el componente (4a, ..., 4d) de control y la segunda información de estado (Z2) contiene información sobre un estado del actuador detectado por el componente (5a, ..., 5d) de monitorización y

- la primera información de estado (Z1) contiene información sobre el estado del componente (4a, ..., 4d) de control y la segunda información de estado (Z2) contiene información sobre un estado del componente (5a, ..., 5d) de monitorización.

2. Sistema (1) de control de acuerdo con la reivindicación 1, en donde la red (3) de comunicación está configurada como una red inalámbrica.

3. Sistema (1) de control de acuerdo con una de las reivindicaciones 1 a 2,

- que presenta, además, al menos un componente (8a, ..., 8d) de detección,

- en donde el componente (8a, ..., 8d) de detección está configurado para detectar un estado del actuador (2a, ... 2d) y transmitir información sobre el estado detectado a al menos uno de los componentes (5a, ..., 5d) de monitorización.

4. Sistema (1) de control de acuerdo con una de las reivindicaciones 1 a 3, en donde los componentes (5a, ..., 5d) de monitorización están configurados para monitorizar el estado del actuador (2a, ..., 2d) sin realimentación y/o independientemente del componente (4a, ..., 4d) de control.

5. Sistema (1) de control de acuerdo con una de las reivindicaciones 1 a 4, en donde

- la red (3) de comunicación se configura utilizando un protocolo de red tolerante a fallos, y

- los componentes (4a, ...,4d) de control y los componentes (5a, ..., 5d) de monitorización están configurados para comunicarse a través del protocolo de red tolerante a fallos de la red (3) de comunicación.

6. Sistema (1) de control de acuerdo con una de las reivindicaciones 1 a 5, en donde el sistema (1) de control es un sistema de señalización/enclavamiento para vehículos ferroviarios.

7. Procedimiento para el funcionamiento de un sistema (1) de control que presenta

- al menos un actuador (2a, ..., 2d),

- una pluralidad m de componentes (4a, ..., 4d) de control,

- una pluralidad n de componentes (5a, ..., 5d) de monitorización,

- una red (3) de comunicación y

- una fuente (7) de alimentación central para suministrar energía eléctrica al sistema (1) de control, en donde una o más informaciones de estado (Zdef) predeterminadas sobre estados definidos del actuador (2a, ..., 2d) y/o el componente de control y/o el componente de monitorización se almacenan en la red de comunicación,

- en donde los componentes (4a, ..., 4d) de control controlan el actuador (2a, ..., 2d) y

- en donde los componentes (5a, ..., 5d) de monitorización monitorizan un estado del actuador (2a, ...,2d), que comprende los siguientes pasos:

- generación (G) de la primera información de estado (Z1) por al menos uno de los componentes (4a, ..., 4d) de control,

- generación (G) de una segunda información de estado (Z2) por al menos uno de los componentes (5a, ..., 5d) de monitorización,

- intercambio (S) de la primera y segunda información de estado (Z1, Z2) entre los componentes (4a, ..., 4d) de control y los componentes (5a, ..., 5d) de monitorización a través de la red (3) de comunicación,

- comparación (E) de la primera y segunda información de estado (Z1, 72) entre sí y/o correspondientemente con la información de estado predeterminada (Zdef) por los componentes (4a, ..., 4d) de control y por los componentes (5a, ..., 5d) de monitorización,

- transferencia (C) del sistema (1) de control por los componentes (4a, ..., 4d) de control y/o por los componentes (5a, ..., 5d) de monitorización a un estado seguro desconectando la fuente (7) de alimentación central, si la comparación (E) de la primera y segunda información de estado (Z1, Z2) entre sí y/o correspondientemente con la información de estado (Zdef) predeterminada da como resultado una desviación de la primera y segunda información de estado (Z1, Z2) entre sí y/o correspondientemente con respecto a la información de estado (Zdef) predeterminada,

en donde

- la primera y segunda información de estado (Z1, Z2) es información combinada sobre los estados del componente (4a, ..., 4d) de control y del componente (5a, ..., 5d) de monitorización y sobre uno o más estados del actuador (2a, ..., 2d), y

- la primera información de estado (Z1) contiene información sobre un estado del actuador (2a... 2d) detectado por el componente (4a, ..., 4d) de control y la segunda información de estado (Z2) contiene información sobre un estado del actuador (2a, ..., 2d) detectado por el componente (5a, ..., 5d) de monitorización, y

- la primera información de estado (Z1) contiene información sobre el estado del componente (4a, ..., 4d) de control y la segunda información de estado (Z2) contiene información sobre un estado del componente (5a, ..., 5d) de monitorización.

8. Procedimiento de acuerdo con la reivindicación 7, en donde

- el sistema (1) de control comprende al menos un componente (8a, ..., 8d) de detección y

- el componente (8a, ..., 8d) de detección detecta un estado del actuador (2a, ..., 2d) y transmite información sobre el estado detectado a al menos uno de los componentes (5a, ..., 5d) de monitorización.

9. Procedimiento de acuerdo con una de las reivindicaciones 7 a 8, en donde los componentes (5a, ..., 5d) de monitorización monitorizan el estado del al menos un actuador (2a, ..., 2d) sin realimentación y/o independientemente del componente (4a, ..., 4d) de control.

10. Procedimiento de acuerdo con una de las reivindicaciones 7 a 9, en donde la red (3) de comunicación se establece mediante un protocolo de red tolerante a fallos y los componentes (4a, ..., 4d) de control y los

componentes (5a, ..., 5d) de monitorización se comunican a través del protocolo de red tolerante a fallos de la red (3) de comunicación.

11. Programa de control que está configurado para ejecutarse dentro de un sistema (1) de control y que, cuando se ejecuta dentro del sistema (1) de control, lleva a cabo un procedimiento de acuerdo con una de las reivindicaciones 7 a 10.

DIBUJOS

FIG 1

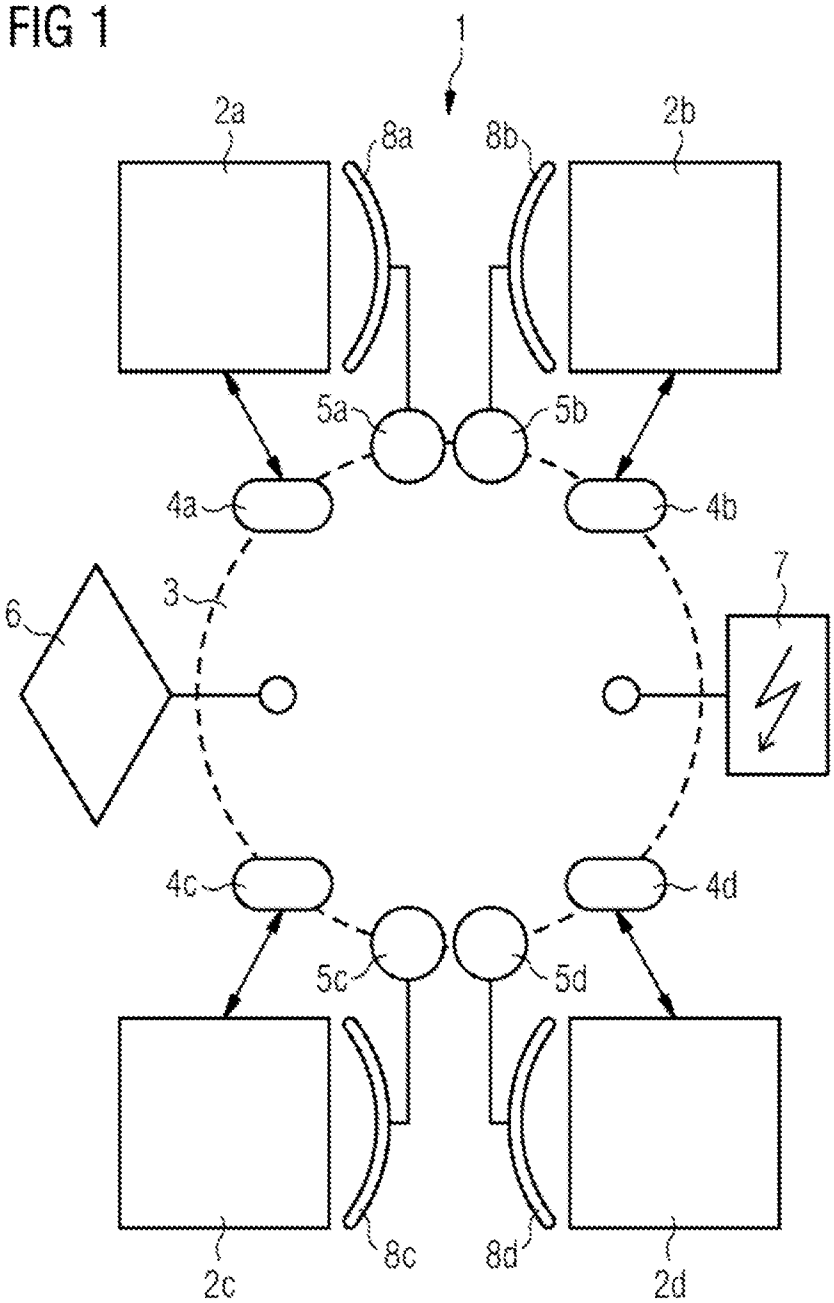


FIG 2

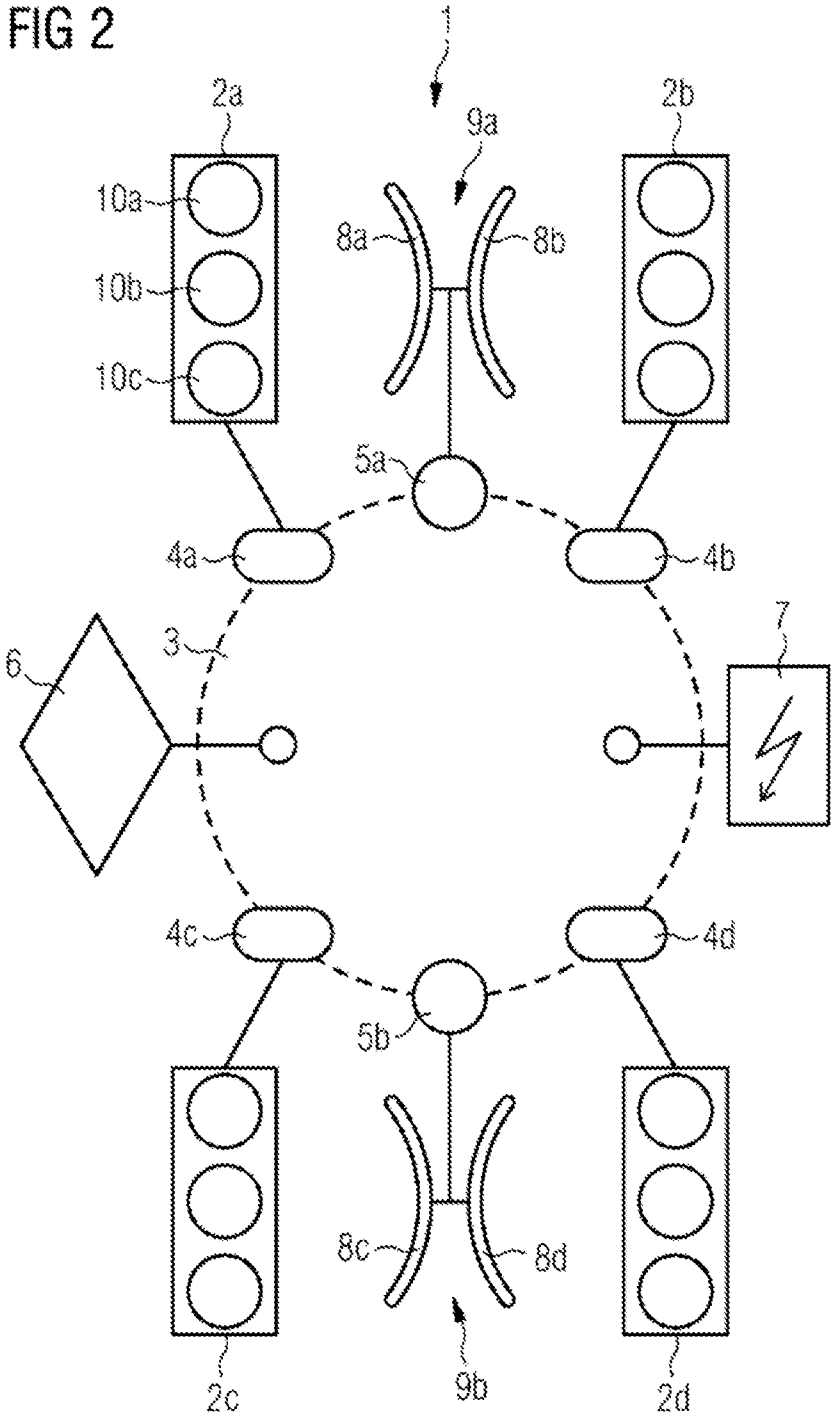


FIG 3

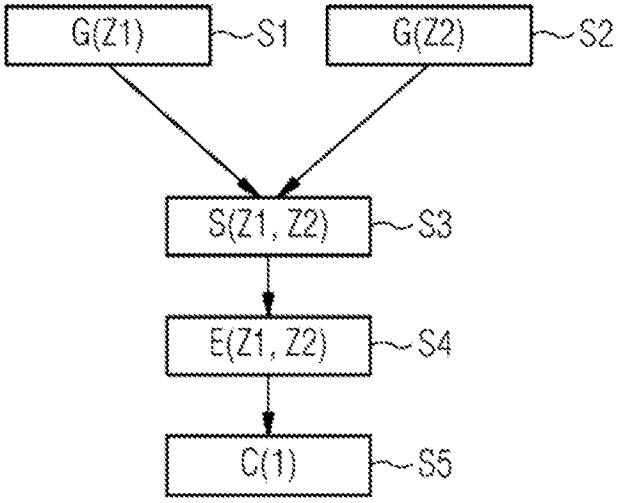
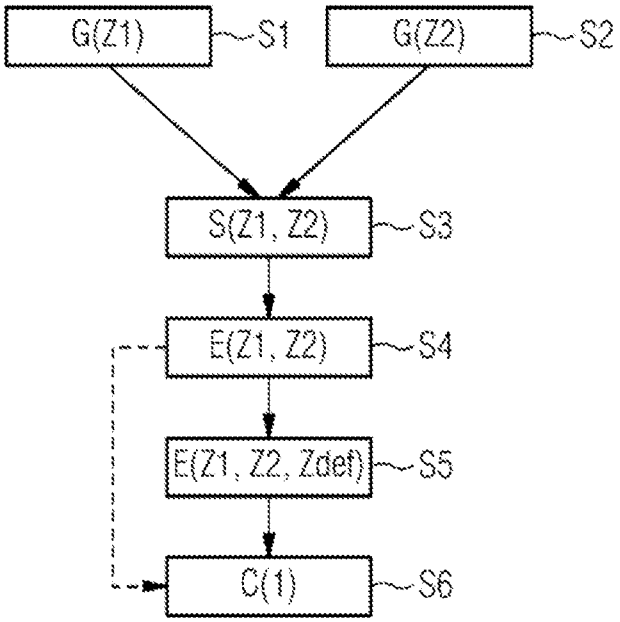

G(Z1)
S1
G(Z2)
S2
S(Z1, Z2)
S3
E(Z1, Z2)
S4
C(1)
S5

FIG 4


G(Z1)
S1
G(Z2)
S2
S(Z1, Z2)
S3
E(Z1, Z2)
S4
E(Z1, Z2, Zdef)
S5
C(1)
S6