

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 970 584**

51 Int. Cl.:

**G05B 19/042** (2006.01)

**G06F 11/07** (2006.01)

**G06F 11/14** (2006.01)

12

## TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **22.09.2020** **PCT/EP2020/076412**

87 Fecha y número de publicación internacional: **01.04.2021** **WO21058471**

96 Fecha de presentación y número de la solicitud europea: **22.09.2020** **E 20776141 (2)**

97 Fecha y número de publicación de la concesión europea: **08.11.2023** **EP 4034949**

54 Título: **Controlador electrónico de potencia programable**

30 Prioridad:

**25.09.2019 DE 102019125867**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:  
**29.05.2024**

73 Titular/es:

**KEBA INDUSTRIAL AUTOMATION GERMANY  
GMBH (100.0%)  
Gewerbestraße 5-9  
35633 Lahnau, DE**

72 Inventor/es:

**WERTZ, HARALD;  
TIEN, PATRICK;  
HERRMANN, GERALD y  
BACH-PRECKWINKEL, HEIKO**

74 Agente/Representante:

**CARVAJAL Y URQUIJO, Isabel**

ES 2 970 584 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

## DESCRIPCIÓN

## Controlador electrónico de potencia programable

La invención se refiere a un controlador electrónico de potencia programable con un módulo de potencia para controlar al menos un actuador, en particular un actuador electromecánico, que puede conectarse o está conectado al módulo de potencia, mediante una señal de control del actuador, por ejemplo, en forma de una tensión aplicada o una corriente seleccionada adecuadamente. La tensión o la corriente puede ser suministrada por una fuente de alimentación adecuada y ajustada en consecuencia en el módulo de potencia del controlador de potencia, por ejemplo, mediante un controlador tiristor, un transformador, un inversor, un modulador de ancho de pulso o un dispositivo electrónico similar, con el que la potencia de salida o la corriente de salida y/o la tensión de salida pueden ajustarse en forma variable.

El actuador de potencia también presenta un módulo de control para accionar o controlar el módulo de potencia mediante una señal de control del módulo de potencia y un módulo de supervisión interno para transferir el módulo de control a un modo de emergencia. En el modo de emergencia, el módulo de control está configurado para ejecutar una respuesta de error predefinida y colocar el actuador en un estado seguro, mientras que el módulo de supervisión interno está configurado para supervisar un estado del sistema, reconocer un estado de funcionamiento crítico y, en caso de que se reconozca un estado de funcionamiento crítico, emitir al menos una señal de error, que en particular coloca el módulo de control o el controlador de potencia en el modo de emergencia.

Tales controladores de potencia programables se utilizan a menudo en sistemas en los que la simple desconexión de uno o más actuadores electromecánicos en caso de fallo (es decir, un estado de funcionamiento crítico) es o puede ser peligrosa, porque hay al menos una fase de funcionamiento crítica del sistema en la que la simple desconexión de los actuadores violaría uno o más objetivos de seguridad del sistema. Una aplicación frecuente y preferida según la invención es un sistema de paso de una turbina eólica, con el que se ajusta la posición rotacional de al menos una pala del rotor en el buje del rotor. Otros ámbitos de aplicación útiles podrían ser los procesos de producción críticos o los vehículos propulsados eléctricamente. En tales sistemas, deben preverse medidas de tolerancia a fallos que permitan al menos el funcionamiento de emergencia del sistema en caso de fallo ("sistema operativo en caso de fallo").

Los controladores electrónicos de potencia programables (PEL) se utilizan casi siempre en actuadores electromecánicos controlados. Además de las funciones básicas propiamente dichas para controlar el actuador, contienen numerosas funciones adicionales, por ejemplo, para la lectura de sensores externos, la generación de perfiles cinemáticos de movimiento y la comunicación en tiempo real con otros sistemas a través de interfaces de comunicación complejas. Otras funciones adicionales permiten, por ejemplo, realizar cómodamente el diagnóstico, la parametrización, la programación del usuario y la puesta en servicio de los controladores electrónicos de potencia programables. La complejidad de estos controladores de potencia programables encierra riesgos significativos de errores de software sistemáticos no detectados.

Los errores de software en las complejas funciones adicionales pueden impedir la transición fiable del controlador de potencia del funcionamiento normal al funcionamiento de emergencia, por ejemplo, si el software se bloquea durante el procesamiento o, por ejemplo, consume mucha potencia del procesador en un bucle sin fin. Cuando se utilizan varios controladores de potencia complejos similares en un sistema, existe un alto riesgo de que se produzcan errores de "causa común" críticos para el sistema. La minimización adecuada de la probabilidad de que se produzcan estos errores de causa común mediante medidas de prevención de errores durante el desarrollo del producto no suele ser posible en la medida suficiente con sistemas complejos, aunque sea por razones de costes.

La integración de la seguridad funcional en el control de actuadores electromecánicos, por ejemplo, en sistemas de accionamiento eléctricos, se conoce desde hace varios años y se ha introducido en la práctica industrial. El estado seguro del actuador suele ser la parada con desconexión segura de la generación de par o fuerza y control seguro del freno. Incluso las funciones de seguridad que pueden solicitarse mientras el movimiento está en marcha, como un par limitado en forma segura, una velocidad limitada en forma segura o un rango de posición limitado en forma segura, siempre incluyen la parada con la consiguiente desconexión del par o la fuerza como una reacción de fallo segura tras la detección de una avería.

Una reacción de error compleja puede ser, en particular, alcanzar una posición segura en un tiempo determinado. Un ejemplo de ello es, por ejemplo, un accionamiento de paso para ajustar el ángulo de las palas del rotor de una turbina eólica. Dependiendo de la aplicación, otras posibles reacciones de error pueden ser el mantenimiento de una velocidad de accionamiento o la reducción/aumento de una velocidad de accionamiento tras una rampa de aceleración o frenado especificada hasta un valor objetivo especificado.

El requisito previo para ejecutar una función de error compleja es que el módulo de control del controlador de potencia pueda seguir controlando en forma fiable esta respuesta de error a pesar del estado de funcionamiento crítico. Sin embargo, esto no es posible si el propio módulo de control deja de funcionar correctamente, por ejemplo, debido a errores de software en funciones adicionales complejas y, por ejemplo, toda la potencia del procesador se consume ejecutando una función adicional que no es importante en términos de seguridad.

El documento DE 10 2012 012 521 A1 describe un controlador programable para aplicaciones críticas de seguridad

en el entorno de una máquina. Se pretende que la función de los componentes del programa relevantes para la seguridad no se vea influida por errores o secuencias de otros componentes del programa. Para el control secuencial de los programas de aplicación pueden utilizarse diversos criterios, por ejemplo, el control secuencial puede basarse en un sistema de tiempo de ejecución junto con un sistema operativo. Existe un funcionamiento paralelo e independiente de un programa normal y de un programa seguro sobre la base de una estructura de sistema de tiempo de ejecución, en la que se propone integrar todos los componentes relevantes para el control en un componente de hardware con una arquitectura de hardware específica y separarlos entre sí mediante una estructura de sistema de tiempo de ejecución con al menos dos sistemas de tiempo de ejecución para poder realizar libremente modificaciones en los componentes no relevantes para la seguridad. La separación puede lograrse, en particular, dando prioridad a uno de los sistemas en tiempo de ejecución.

El documento DE 10 2005 007 477 A1 describe un controlador programable para la automatización de máquinas y/o sistemas con un controlador estándar con funciones de control estándar y un controlador de seguridad con funciones de seguridad basado en un PC. El controlador de seguridad consiste en uno o más módulos de seguridad conectados al bus del PC, y en los módulos de seguridad se prevé firmware con certificación de seguridad. La unidad de control proporciona así una separación entre la función estándar no relacionada con la seguridad y la función de seguridad mediante una división modular dentro de la unidad de control. Con esta división, la función estándar no está sujeta a ninguna restricción relacionada con la seguridad y puede realizarse de una manera correspondientemente compleja.

El documento US 2013/231767 A1 describe un módulo multichip que contiene un primer chip con un procesador de control para generar una señal para controlar un proceso industrial y una interfaz de entrada/salida. El módulo multichip también comprende un segundo chip con un procesador de monitorización y una interfaz de entrada/salida. Un fallo del procesador de control o del procesador de supervisión es reconocido por el otro procesador. El procesador que reconoce el fallo está configurado para emitir una señal a través de su interfaz de entrada/salida con el fin de permitir que el proceso industrial pase a un estado seguro en respuesta al fallo.

Con este trasfondo, la tarea de la invención es proporcionar un controlador electrónico de potencia programable con el que las reacciones de error complejas sean procesadas en forma fiable por el módulo de control incluso en un estado de funcionamiento crítico, con el fin de llevar el sistema a una parada segura en forma definida.

Esta tarea se resuelve con un controlador electrónico de potencia programable del tipo mencionado al principio, en particular en el sentido de que el módulo de control del controlador electrónico de potencia programable presenta una unidad de control básica, una unidad de control adicional y una interfaz de control. En particular, el módulo de control puede constar de estos tres componentes.

La unidad de control básica está configurada para emitir las señales de control del módulo de potencia. Además, la unidad de control básica implementa las o, preferiblemente, todas las funciones de control autónomo y regulación del actuador que son necesarias para el funcionamiento de emergencia en un estado de funcionamiento crítico. La unidad de control básica es, por lo tanto, la parte del módulo de control que controla el actuador (es decir, emite las señales de control del módulo de potencia). El módulo de potencia proporciona entonces la potencia necesaria para el actuador en forma de una señal de control del actuador. En particular, la señal de control del actuador puede ser una señal de corriente y/o tensión con la que se alimenta el actuador, por ejemplo, un motor trifásico.

Las funciones implementadas para el control y la regulación autónomos del actuador incluyen, en particular, instrucciones para convertir órdenes de posicionamiento (lógicas) procedentes de un sistema de control y/o regulación en señales de control (orientadas a la máquina) del módulo de potencia, así como los algoritmos de control y regulación del actuador y los sensores necesarios para ello.

En el caso de un accionamiento de paso de una turbina eólica para el ajuste giratorio de una de las palas del rotor en un buje del rotor como aplicación preferida, el actuador electromecánico puede ser en particular un accionamiento trifásico (motor trifásico). En este caso, la unidad de control básica para el control y la regulación autónomos del accionamiento trifásico comprende en particular una adquisición de valores de medición, un modelo de campo (que se utiliza, por ejemplo, para describir el estado del actuador o del sistema controlado por el actuador, generalmente sobre la base de los valores de medición adquiridos), un control de corriente, una modulación y un control de velocidad.

Las funciones que no son necesarias para el funcionamiento de emergencia en un estado de funcionamiento crítico se implementan en el sistema de control adicional. Puede tratarse de funciones como el análisis de sensores externos, la generación de perfiles cinemáticos de movimiento o la comunicación en tiempo real con sistemas externos a través de interfaces de comunicación (a veces complejas). Tales funciones son especialmente útiles y deseables para optimizar el funcionamiento del sistema controlado por el actuador, sin ser relevantes para la seguridad. Otras funciones adicionales permiten, por ejemplo, realizar cómodamente el diagnóstico, la parametrización, la programación por el usuario y la puesta en servicio del controlador electrónico de potencia programable, y simplifican el mantenimiento y la revisión.

Como elemento opcional, el controlador electrónico de potencia propuesto puede, por lo tanto, estar conectado o ser conectable a un controlador externo a través de una interfaz de la unidad de control adicional de acuerdo con la invención. De acuerdo con la invención, la unidad de control adicional puede configurarse para enviar datos de

funcionamiento de la unidad de control adicional al controlador externo y/o para recibir datos de control del controlador externo.

La interfaz de control prevista según la invención conecta la unidad de control básica con la unidad de control adicional a través de una conexión de control, que puede comprender tanto una conexión de control de la unidad de control básica a la unidad de control adicional como una conexión de control de la unidad de control adicional a la unidad de control básica. En funcionamiento normal, la conexión de control permite que la unidad de control básica y la unidad de control adicional se utilicen conjuntamente e intercambien datos entre sí. Esto significa que, en el funcionamiento normal, pueden ejecutarse tanto las funciones que (también) son necesarias en el funcionamiento de emergencia y que están implementadas en la unidad de control básica, como las funciones que solo pueden ejecutarse en el funcionamiento normal y que están implementadas en la unidad de control adicional.

En caso de error, es decir, cuando el módulo de control interno reconoce un estado de funcionamiento crítico, el punto de desconexión de control está configurado para recibir la señal de error de la señal de control interno y, tras recibirla, desconectar la conexión de control al menos parcialmente, por ejemplo, en una dirección de conexión de la conexión de control de la unidad de control básica a la unidad de control adicional o en una segunda dirección de conexión de la conexión de control de la unidad de control adicional a la unidad de control básica, pero preferiblemente por completo en ambas direcciones de conexión. En otras palabras, el módulo de control según la invención está configurado para separar funcionalmente la unidad de control básica de la unidad de control adicional en funcionamiento de emergencia, de modo que se pueda descartar la influencia externa de la unidad de control básica por parte de la unidad de control adicional.

El controlador electrónico de potencia programable según la invención puede utilizarse, por lo tanto, para implementar un procedimiento, también según la invención, con el que se realiza un control seguro del actuador en el módulo de control, en el que, tras detectarse un fallo de funcionamiento, se pasa a un funcionamiento de emergencia con una gama reducida de funciones, en el que la unidad de control básica ejecuta en forma autónoma una reacción compleja ante errores sin ser influido y/o accedido por una unidad de control adicional, antes de que el actuador se detenga en forma segura como es habitual en el estado de la técnica. Según la invención, es posible prescindir de la ejecución de una evaluación de errores en el software durante el funcionamiento de emergencia. Dicha evaluación de errores es generalmente compleja y sirve en particular para detectar y mostrar sistemáticamente los fallos de funcionamiento antes de que se alcance un estado de funcionamiento crítico. Esto permite corregir errores sistemáticos mediante actualizaciones del software y/o contrarrestar de antemano el desarrollo de un estado de funcionamiento crítico. Una vez alcanzado el estado de funcionamiento crítico, la atención se centra en la ejecución de una función de error compleja. Por lo tanto, se puede implementar una evaluación de errores (exhaustiva) en la unidad de control adicional según la invención y, por lo tanto, no estar disponible en el funcionamiento de emergencia.

En el contexto de la invención, se reconoció que los problemas en el funcionamiento de emergencia se producen en particular cuando las partes de software para las funciones básicas y las funciones adicionales se ejecutan en el mismo microcontrolador con recursos compartidos (CPU, periféricos, memoria). Para evitar este problema, las distintas partes del sistema de control se han dividido en un sistema de control básico -autosuficiente- y un sistema de control adicional, en el que se ha previsto una interfaz de control fiable para separar en forma segura los dos sistemas de control parciales entre sí, especialmente en caso de fallo crítico. De este modo, la solución descrita en la presente invención permite un funcionamiento de emergencia con una gama reducida de funciones mediante la separación del complejo hardware y software de control en una unidad de control básica y una unidad de control adicional por medio de un módulo de supervisión independiente. La unidad de control básica solo contiene los componentes de hardware y software necesarios para el reducido alcance de funciones del funcionamiento de emergencia, que son significativamente menos complejos en conjunto que los de la unidad de control adicional. Esto tiene la ventaja de que la evaluación relacionada con la seguridad del software del control del actuador (es decir, el módulo de control) puede limitarse al software de la unidad de control básica y, por lo tanto, es mucho más sencilla que la evaluación del software de control completo.

La separación entre la unidad de control básica y la unidad de control adicional puede llevarse a cabo en una realización sencilla implementando una interfaz preferiblemente bidireccional entre las dos unidades de control, que permita una conexión de control (en el sentido de un enlace de comunicación) entre las dos unidades de control de modo que puedan intercambiarse datos entre las dos unidades de control. En tal caso, la unidad de control básica puede desconectarse de la unidad de control adicional interrumpiendo la interfaz de comunicación.

En otra realización, que puede llevarse a cabo alternativa o adicionalmente, la interfaz de control puede implementarse como un dispositivo de protección de memoria, que se configura para proteger áreas de memoria definidas de la unidad de control básica de la influencia de la unidad de control adicional. Por ejemplo, se puede implementar una restricción de acceso (por ejemplo, una restricción de escritura, posiblemente incluso junto con una restricción de lectura) para acceder a las áreas de memoria de la unidad de control básica. Esto también evita que un problema de software en la unidad de control adicional afecte a la unidad de control básica. Esto también se entiende como desconexión de la conexión de control entre la unidad de control básica y la unidad de control adicional.

En una realización adicional, alternativa o complementaria, la interfaz de control puede configurarse para que la unidad de control adicional pase a un estado de restablecimiento cuando se reciba la señal de error del módulo de control

interno y se mantenga así hasta que finalice el funcionamiento de emergencia. En el estado de restablecimiento, la unidad de control adicional no tiene ningún efecto sobre el controlador de potencia, de modo que la unidad de control básica no puede verse influida por la unidad de control adicional. De este modo, también se desconecta la conexión de control entre la unidad de control básica y la unidad de control adicional.

5 De acuerdo con una realización preferida del controlador de potencia propuesto según la invención, el módulo de control puede presentar varios procesadores, por lo que la unidad de control básica y la unidad de control adicional se implementan cada una en procesadores diferentes. Por lo tanto, se prevé al menos un procesador separado tanto para la unidad de control básica como para la unidad de control adicional. Esto significa que la separación de la unidad de control básica y la unidad de control adicional también se puede realizar en el lado del hardware. En caso necesario,  
10 el procesador con la unidad de control adicional puede desconectarse o desactivarse en modo de emergencia para evitar cualquier influencia de la unidad de control adicional en la ejecución de las reacciones de error complejas y separar, de este modo, la conexión de control entre la unidad de control básica y la unidad de control adicional.

En una realización similar de la invención, el módulo de control puede tener un procesador multinúcleo, en el que la unidad de control básica y la unidad de control adicional se implementan cada una en al menos un núcleo diferente del procesador multinúcleo. De este modo, también se consigue una separación de la conexión de control entre la  
15 unidad de control básica y la unidad de control adicional en el lado del hardware.

Como característica de seguridad adicional, el módulo de potencia según la invención puede presentar un punto de desconexión del módulo de potencia, que está dispuesto entre el módulo de potencia y una conexión al actuador y está configurado para recibir la señal de error del módulo de control interno y, tras recibirla, no transmitir la señal de control del actuador a la conexión del actuador (sinónimo de: no al actuador o a varios actuadores). Esto corresponde  
20 aproximadamente a una función de parada de emergencia que desenergiza la conexión al actuador, es decir, detiene instantáneamente el actuador. En este caso, ya no se puede ejecutar la respuesta compleja a errores según la invención. Tal caso puede ocurrir posiblemente después del fallo de componentes de hardware críticos que ya no permiten la operación de emergencia del actuador de potencia. En este caso, puede ser útil apagar los actuadores electromecánicos inmediatamente.  
25

En este caso, el módulo de control interno puede desconectar uno o más componentes conectados externamente del controlador de potencia activando el punto de desconexión del módulo de potencia mediante una señal de error al punto de desconexión del módulo de potencia (como un segundo nivel de reserva para la gestión de errores, por así decirlo). De este modo, puede evitarse un flujo de energía entre los componentes conectados externamente y el  
30 controlador de potencia. Los múltiples componentes pueden ser diferentes actuadores que realizan diferentes procesos de actuación y pueden ser tratados por separado o conjuntamente por el controlador de potencia. Los posibles actuadores pueden ser motores, un freno de mantenimiento u otros dispositivos accionados eléctricamente. Un freno de mantenimiento puede, por ejemplo, realizarse de tal manera que requiera una fuente de alimentación para abrir el freno y lo cierre cuando se retire la fuente de alimentación.

35 Otros componentes conectados al módulo de potencia pueden ser una fuente de alimentación, por ejemplo, una fuente de alimentación de red o una unidad de almacenamiento de energía. La activación del punto de desconexión del módulo de potencia puede, preferiblemente, desconectar también la fuente de alimentación del módulo de potencia del controlador de potencia y apagar así todos los actuadores conectados.

Los componentes individuales pueden separarse selectivamente, en grupos o juntos.

40 En una realización particularmente preferida de la invención, un dispositivo de señalización interno, un transmisor de señales externo y/o un módulo de monitorización externo pueden conectarse al módulo de supervisión interno, por lo que el dispositivo de señalización interno, el transmisor de señales externo y/o el módulo de monitorización externo están configurados para enviar señales de datos al módulo de supervisión interno. Los dispositivos de señalización interno y externo pueden ser, por ejemplo, transductores con sensores que transmiten las señales de los sensores y/o  
45 los valores de los sensores derivados de las señales de los sensores como señales de datos. El módulo de supervisión externo puede ser un módulo de seguridad independiente para reconocer situaciones de fallo o peligro, que recopila y evalúa información en forma independiente (valores de medición, valores de estado u otros datos). Una señal de error, por ejemplo, puede enviarse entonces al módulo de control interno como señal de datos. Esta señal de error puede entenderse como una señal de solicitud al módulo de supervisión interno para transferir el controlador electrónico de potencia programable a un modo de emergencia en el que, según la invención, la unidad de control básica se desconecta de la unidad de control adicional (ejecución de una reacción de error compleja) y/o para desconectar el módulo de potencia de los actuadores conectados, de la fuente de alimentación y/o de otros componentes de potencia conectados (apagado del componente, en particular en el sentido de una parada de emergencia).  
50

55 Además, la unidad de control básica puede conectarse directamente al módulo de monitorización interna y enviar señales de datos al módulo de monitorización interna. Una posibilidad para dicha señal de datos es una señal de error. Esta señal de error también puede entenderse como una señal de solicitud al módulo de control interno para transferir el controlador electrónico de potencia programable al modo de emergencia, por ejemplo, si se reconoce un estado del controlador básico y/o (también en funcionamiento normal) del controlador adicional en el controlador básico que es

crítico y que posiblemente podría provocar un fallo del controlador básico y/o adicional.

En respuesta a la evaluación, si el módulo de control interno reconoce una situación de funcionamiento crítica, el módulo de control interno puede emitir una o varias señales de error. La detección de una situación de funcionamiento crítica puede determinarse, por ejemplo, comparando las señales de datos recibidas con intervalos admisibles. También es posible combinar varios valores de datos, posiblemente utilizando reglas algebraicas, procedimientos de lógica difusa o inteligencia artificial (IA).

El módulo de control interno también puede reconocer diferentes niveles de estados críticos de funcionamiento y, en función del nivel detectado, emitir diferentes señales de error. A continuación, se explican varias posibilidades de señales de error. Todas estas señales de error pueden enviarse individualmente o en cualquier combinación, si es necesario, además de la señal de error ya descrita a la interfaz de control.

En una realización ventajosa según la invención, el módulo de control interno puede configurarse para enviar una señal de error (señal de error de reinicio) a la unidad de control básica, por lo que la unidad de control básica está configurado para activar un reinicio de la unidad de control básica cuando se recibe esta señal de error. Si el controlador de potencia eléctrica programable complejo falla durante un estado crítico del sistema, se puede activar el funcionamiento de emergencia mediante un reinicio por software del controlador del actuador.

De acuerdo con una variante preferida, el reinicio se realiza de tal manera que el módulo de control funciona automáticamente en modo de emergencia tras el reinicio debido a la señal de error de reinicio, es decir, la unidad de control básica se desconecta de la unidad de control adicional. Preferiblemente, todo el sistema de control puede desconectarse durante el reinicio y solo puede arrancarse el sistema de control básico. Esto permite que el reinicio se realice tan rápido como lo requiera el tiempo de respuesta de seguridad del sistema. Tras el reinicio, el software funciona automáticamente en modo de emergencia, en el que las complejas funciones adicionales del controlador programable de energía eléctrica que no son necesarias se desactivan en forma fiable. Esto elimina la influencia potencialmente peligrosa de los errores sistemáticos de software en las funciones adicionales complejas sobre la disponibilidad de las funciones básicas necesarias para el funcionamiento de emergencia. Por ejemplo, la unidad de control adicional puede mantenerse en el estado de restablecimiento descrito con anterioridad hasta que deje de existir la situación de funcionamiento crítica.

Una ventaja especial de esta variante según la invención es que el controlador básico trabaja en un estado de funcionamiento definido después del reinicio rápido y se pueden ejecutar en forma fiable reacciones de error complejas.

De acuerdo con otra variante, el módulo de control interno puede estar configurado para enviar una señal de error a la unidad de control básica, de modo que la unidad de control básica esté configurada para prepararse para un funcionamiento de emergencia cuando se reciba esta señal de error (señal de error de preaviso). Esta señal de error de preaviso puede ser enviada por el módulo de control interno en una fase muy temprana, por ejemplo, si existe una indicación de un posible estado de funcionamiento crítico en el módulo de control interno, por ejemplo, sin que se haya confirmado completamente en el módulo de control interno. Dicha señal de error de preaviso puede utilizarse, por ejemplo, en la unidad de control básica para comprobar el estado de funcionamiento de la unidad de control básica, para cancelar funciones ejecutadas a petición de la unidad de control adicional y/o para enviar una señal de datos al módulo de control interno que indique que es útil o necesario reiniciar la unidad de control básica. Dicha señal de error de preaviso puede utilizarse para iniciar una transición ordenada al funcionamiento de emergencia.

De acuerdo con la invención, puede enviarse otra señal de fallo al módulo de supervisión externo para transmitir la aparición de un estado de funcionamiento crítico, por ejemplo, a un centro de control para que emita una alerta. El módulo de supervisión externo también puede ser el módulo o módulos de control interno de uno o más controladores eléctricos programables instalados en el mismo sistema. Esto permite conectar en red diferentes controladores de potencia del mismo sistema. Esto es ventajoso porque las situaciones críticas de funcionamiento reconocidas para otro controlador de potencia, en particular las causadas por influencias ambientales, a menudo también se aplican a los otros controladores de potencia del mismo sistema. Gracias a este tipo de conexión en red, esto puede detectarse rápidamente en todo el sistema.

Además de la señal de error después de que se haya producido el estado de funcionamiento crítico o se haya iniciado el funcionamiento de emergencia, también se puede enviar al módulo de supervisión externo una señal de error de preaviso como la descrita con anterioridad.

En una realización especialmente preferida, solo la unidad de control básica puede configurarse para emitir señales de control del módulo de potencia al módulo de potencia y/o para ejecutar otras funciones (esenciales) del módulo de control. Esto significa que las funciones esenciales de la unidad de control básica, en particular las funciones asociadas con el control directo del actuador, son controladas exclusivamente por la unidad de control básica tanto en funcionamiento normal (es decir, con la unidad de control básica y la unidad de control adicional activas) como en funcionamiento de emergencia (es decir, solo con la unidad de control básica activa y la unidad de control adicional desactivada/desactivada). Por lo tanto, cabe suponer que estas funciones también se ejecutan sin errores en el modo de emergencia. En otras palabras, al menos una gran parte de las funciones necesarias en el modo de emergencia

también están constantemente en funcionamiento o en uso durante el funcionamiento normal. Por lo tanto, estas funciones pueden considerarse probadas.

5 Con el fin de cancelar también de nuevo una operación de emergencia si, por ejemplo, ya no existe un estado de funcionamiento crítico, el dispositivo de control interno puede configurarse de acuerdo con la invención para reconocer el final de una operación de emergencia y transferir el controlador electrónico de potencia programable de operación de emergencia a operación normal, en particular desactivando el punto de desconexión de control y/o el punto de desconexión del módulo de potencia.

10 Ventajosamente, el dispositivo de monitorización interna puede ser una unidad funcional autosuficiente del controlador electrónico de potencia programable que puede funcionar independientemente del módulo de control. En otras palabras, esto significa que la unidad de monitorización interna del controlador de potencia en esta realización también es funcional cuando ni el módulo de control ni el módulo de potencia están activados. Esta autosuficiencia con respecto a las demás unidades funcionales del controlador de potencia garantiza una función de seguridad fiable. De este modo, el módulo de control interno también puede asumir una función de vigilancia y comprobar el funcionamiento de la unidad de control básica en particular, por ejemplo, mediante la consulta de determinados datos de estado en forma casi continua. Si los datos de estado no se materializan, el módulo de control interno puede activar un reinicio de todo el módulo de control en funcionamiento normal o un reinicio solo de la unidad de control básica en funcionamiento de emergencia.

20 La invención también se refiere a un uso especialmente ventajoso del controlador electrónico de potencia programable propuesto para controlar un sistema de paso de una turbina eólica, con el que se ajusta la posición rotacional de una o más palas del rotor en el buje del rotor. Se trata de una aplicación especialmente relevante desde el punto de vista de la seguridad, ya que, por ejemplo, en caso de tormenta o de fuertes ráfagas de viento, las palas del rotor de la turbina eólica deben moverse a una posición de álabe en la que el viento que fluye contra las palas del rotor solo transfiera una pequeña fuerza a las palas del rotor, a fin de evitar que las palas del rotor se caigan del buje del rotor de la turbina eólica en el peor de los casos.

25 Sin embargo, también es posible un uso ventajoso en otras aplicaciones, por ejemplo, para garantizar el funcionamiento ininterrumpido de actuadores en procesos de producción críticos, por ejemplo, químicos, en accionamientos de tracción eléctrica o en otras aplicaciones en las que la simple desconexión de los actuadores (parada de emergencia) puede dar lugar a situaciones especialmente peligrosas.

30 Otras ventajas, características y posibles aplicaciones de la invención también se desprenden de la siguiente descripción de las realizaciones y del dibujo. Todas las características descritas y/o ilustradas pertenecen juntas o en cualquier combinación que tenga sentido en la técnica para el objeto de la invención, incluso independientemente de su resumen en las realizaciones descritas o ilustradas o en las reivindicaciones.

La Figura 1 muestra un controlador 200 electrónico de potencia programable en una representación esquemática de sus componentes funcionales.

35 El controlador 200 electrónico de potencia programable comprende un módulo 10 de potencia, que está conectado a una fuente 100 de alimentación de red a través de una conexión 101 de potencia y/o a un almacenamiento 90 de energía a través de una conexión 91 de potencia -por ejemplo, para un fallo de alimentación. El módulo 10 de potencia controla un actuador 80 conectado al controlador 200 de potencia a través de una señal 81 de control del actuador.

40 El módulo 10 de potencia es controlado por un módulo 20 de control de acuerdo con la señal 29 de control del módulo de potencia. Los datos de estado del módulo 10 de potencia se envían al módulo 20 de control de acuerdo con la señal 15 de realimentación.

45 Para que el módulo 20 de control pueda procesar en forma fiable reacciones de error complejas incluso en situaciones de funcionamiento críticas y llevar el sistema a una parada segura en forma definida, el controlador 200 electrónico de potencia programable dispone de un módulo 30 de supervisión interno de funcionamiento autónomo, que está configurado para reconocer y evaluar un estado de funcionamiento crítico.

Para la evaluación, el módulo 30 de supervisión interno recibe señales 41 de datos de un transmisor 40 de señales interno. En particular, el transmisor 40 de señales interno puede incluir sensores que detectan valores de estado, como una temperatura, en el controlador 200 de potencia y los envían como señales 41 de datos al módulo 30 de supervisión interno.

50 Del mismo modo, los sensores externos de un transmisor 70 de señales externo, es decir, conectados fuera del controlador 200 de potencia, están conectados al módulo 30 de supervisión interno y envían los valores de estado detectados al módulo 30 de supervisión interno a través de una señal 71 de datos.

55 El módulo 30 de supervisión interno recibe otra señal 51 de datos de un módulo 50 de supervisión externo, que puede, por ejemplo, detectar y evaluar influencias ambientales externas sobre el sistema influido por el actuador. Si estas influencias ambientales externas indican un estado peligroso para el sistema influido por el actuador 80, el módulo 50 de supervisión externo envía una señal 51 de datos, que debe entenderse como una señal de solicitud para que el

módulo 30 de supervisión interno reconozca un estado de funcionamiento peligroso.

Las señales 41, 71, 51 de datos recibidas por el módulo 30 de supervisión interno son registradas y analizadas por el software. Si el módulo 30 de supervisión interno detecta un estado de funcionamiento crítico, pone el módulo 20 de control en modo de emergencia enviando una señal 31 de error.

- 5 A diferencia de una función de parada de emergencia pura, la operación de emergencia del módulo 20 de control también debe realizar una respuesta de error compleja y actuar sobre el actuador 80 a través de la señal 29 de control del módulo de potencia en forma adecuada para llevar el sistema a una parada segura definida. En el módulo 20 de control, pueden introducirse reglas sobre cómo debe ser concretamente esta respuesta de error compleja, por ejemplo, programando adecuadamente determinadas secuencias de proceso.
- 10 Debido a que los sistemas de control complejos con una amplia gama de funciones y, en particular, los sistemas de control programables son susceptibles a errores de software o fallos de funcionamiento, pero, por otro lado, las funciones relevantes para la seguridad deben ejecutarse en forma fiable, se propone una división del sistema de control en el módulo 20 de control en una unidad 21 de control básica y una unidad 23 de control adicional de acuerdo con la invención.
- 15 La unidad 21 de control básica contiene los componentes de hardware y software necesarios para la gama reducida de funciones del funcionamiento de emergencia. En particular, esto incluye la conexión para la salida de la señal 29 de control del módulo de potencia, así como las conexiones para las señales 42, 72 de datos del transmisor 40 de señales interno y del transmisor 70 de señales externo. Los valores de los sensores registrados por estos transmisores 40, 70 de señales en general también son necesarios para procesar la compleja respuesta a fallos.
- 20 La unidad 23 de control adicional contiene funciones adicionales que no son necesarias para el funcionamiento de emergencia, por ejemplo, para analizar sensores externos en un controlador 60 externo, para generar perfiles de movimiento cinemáticos y para la comunicación en tiempo real con sistemas externos (por ejemplo, el controlador 60 externo) a través de interfaces de comunicación (complejas). El controlador 60 externo recibe una señal 26 de datos con datos de funcionamiento de la unidad de control (recepción de datos de funcionamiento enviados por la unidad 23 de control adicional) y envía una señal 61 de datos con datos de control externos (envío de datos por el controlador 60 externo que recibe la unidad 23 de control adicional).
- 25

Otras funciones adicionales de unidad 23 de control adicional permiten, por ejemplo, realizar cómodamente el diagnóstico, la parametrización, la programación del usuario y la puesta en servicio del controlador 200 electrónico de potencia programable.

- 30 Para evitar fallos en la ejecución de funciones de la unidad 21 de control básica por parte de la unidad 23 de control adicional, por ejemplo, debido a errores de software, sin que todo el software de la unidad de control adicional tenga que someterse a una costosa comprobación de seguridad, el módulo 200 de control dispone de una interfaz 22 de control, que está dispuesta en una conexión 24 de control desde la unidad 21 de control básica a la unidad 23 de control adicional y en la conexión 25 de control desde la unidad 23 de control adicional a la unidad 21 de control básica y que puede ser activada por el módulo 30 de supervisión interno para establecer una operación de emergencia mediante una señal 31 de error. La activación de la interfaz 22 de control impide que la unidad 23 de control adicional acceda a la unidad 21 de control básica. Esto puede realizarse técnicamente de diversas maneras, por ejemplo, impidiendo el acceso a la memoria de la unidad 21 de control básica por parte de la unidad 23 de control adicional, colocando la unidad 23 de control adicional en un estado desactivado o de reinicio (es decir, apagando virtualmente la unidad 23 de control adicional), desconectando un enlace de comunicación entre la unidad 21 de control básica y la unidad 23 de control adicional, que están implementadas, por ejemplo, en procesadores separados y conectadas entre sí mediante un enlace de comunicación, o medidas similares técnicamente adecuadas.
- 35
- 40

- 45 Se trata de una forma muy eficaz de limitar las funciones del módulo 20 de control a las necesarias en caso de emergencia y evitar errores en la operación de emergencia debidos a funciones complejas de la unidad 23 de control adicional.

- El módulo 30 de supervisión interno también puede enviar una señal 32 de error a la unidad 21 de control básica, que activa un reinicio de la unidad 21 de control básica en modo de emergencia y, preferiblemente, la desactivación simultánea de la unidad de control adicional (señal de error de reinicio). Técnicamente, esto puede realizarse, por ejemplo, mediante una desconexión rápida de todo el módulo 20 de control con la unidad 21 de control básica y la unidad 23 de control adicional y un reinicio selectivo de la unidad 21 de control básica. Además, el módulo 30 de supervisión interno puede, en caso necesario también con antelación, enviar una señal 33 de error para preavisar una operación de emergencia (señal de error de preaviso). De este modo, la unidad 21 de control básica puede prepararse para el funcionamiento de emergencia.
- 50

- También puede estar previsto que la unidad 21 de control básica, por ejemplo, si detecta un estado inestable de la unidad 23 de control adicional y/o de la unidad 21 de control básica, transmita una señal 28 de datos con esta información al módulo 30 de supervisión interno para su evaluación, que evalúa esta información y, a continuación, inicia el funcionamiento de emergencia de la manera descrita, si es necesario.
- 55

- En función del tipo de estado de funcionamiento detectado por el módulo 30 de supervisión interno, también puede ser necesaria una parada de emergencia inmediata del actuador 80 o de todo el sistema, en lugar de una compleja respuesta a fallos para la desconexión controlada del actuador 80. En una realización preferida, el módulo 30 de supervisión interno puede lograr esto sin la participación de la unidad 21 de control básica por medio de una señal 34 de error a un punto de desconexión del módulo 11 de potencia, que está configurado para desconectar selectivamente ciertas o todas las entradas de potencia de una fuente de alimentación (fuente 100 de alimentación, almacenamiento 90 de energía) y desconectar selectivamente ciertas o todas las salidas de potencia a uno o más actuadores 80 (solo se muestra un actuador en la Figura para simplificar) cuando se activa por la señal 34 de error. De este modo, se realiza una función clásica de parada de emergencia.
- 10 En caso de que se inicie una operación de emergencia y/o para avisar con antelación, el módulo 30 de supervisión interno también puede enviar una señal 36 de error al módulo 50 de supervisión externo, que puede ser un centro de control o estar conectado a un centro de control, por ejemplo.

Lista de símbolos de referencia:

- 10 Módulo de potencia
- 15 11 Punto de desconexión del módulo de potencia
- 15 Señal de realimentación
- 20 Módulo de control
- 21 Unidad de control básica
- 22 Interfaz de control
- 20 23 Unidad de control adicional
- 24 Conexión de control de la unidad de control básica a la unidad de control adicional
- 25 Conexión de control de la unidad de control adicional a la unidad de control básica
- 26 Señal de datos con datos de funcionamiento
- 28 Señal de datos con datos de funcionamiento
- 25 29 Señal de control del módulo de potencia
- 30 Módulo de supervisión interno
- 31 Señal de error a la interfaz de control
- 32 Señal de error a la unidad de control básica para el reinicio (señal de error de reinicio)
- 33 Señal de error a la unidad de control básica para preaviso (señal de error de preaviso)
- 30 34 Señal de error al punto de desconexión del módulo de potencia
- 36 Señal de error al módulo de supervisión externo
- 40 Transmisor de señales interno
- 41 Señal de datos
- 42 Señal de datos
- 35 50 Módulo de control externo
- 51 Señal de datos
- 60 Unidad de control externa
- 61 Señal de datos con datos de control externos
- 70 Transmisor de señales externo

- 71 Señal de datos
- 72 Señal de datos
- 80 Actuador electromecánico
- 81 Señal de control del actuador
- 5 90 Almacenamiento de energía
- 91 Conexión a la red
- 100 Alimentación de red
- 101 Conexión por cable
- 200 Controlador electrónico de potencia programable

## REIVINDICACIONES

1. Controlador electrónico de potencia programable con un módulo (10) de potencia para controlar al menos un actuador (80) que puede conectarse al módulo (10) de potencia mediante una señal (81) de control del actuador, con un módulo (20) de control para accionar el módulo (10) de potencia mediante una señal (29) de control del módulo de potencia y con un módulo (30) de supervisión interno para transferir el módulo (20) de control a un modo de emergencia, en el que el módulo (20) de control está configurado para ejecutar una respuesta de error predefinida y colocar el actuador (80) en un estado seguro, en donde el módulo (30) de supervisión interno está configurado para supervisar un estado del sistema, detectar un estado de funcionamiento crítico y emitir al menos una señal (31, 32, 33, 34, 36) de error, caracterizado porque el módulo (20) de control comprende
  - una unidad (21) de control básica, configurada para emitir las señales (29) de control del módulo de potencia y en la que se implementan las funciones de control y regulación del actuador (80), necesarias para el funcionamiento de emergencia en un estado de funcionamiento crítico,
  - una unidad (23) de control adicional en la que se implementan funciones no necesarias para el funcionamiento de emergencia en un estado de funcionamiento crítico, y
  - un punto (22) de desconexión de control que conecta la unidad (21) de control básica con la unidad (23) de control adicional a través de una conexión (24, 25) de control y está configurado para recibir la señal (31) de error del módulo (30) de supervisión interno y, tras recibirla, desconectar al menos parcialmente la conexión (24, 25) de control,
 en donde el módulo (30) de supervisión está configurado para llevar a cabo una desconexión funcional de la unidad (21) de control básica de la unidad (23) de control adicional en funcionamiento de emergencia, de modo que pueda descartarse una influencia externa de la unidad (21) de control básica por parte de la unidad (23) de control adicional.
2. Controlador electrónico de potencia programable de acuerdo con la reivindicación 1, caracterizado porque la interfaz (22) de control está implementada como un dispositivo de protección de memoria que está configurado para proteger áreas de memoria definidas de la unidad (21) de control básica de ser influenciadas por la unidad (23) de control adicional.
3. Controlador electrónico de potencia programable de acuerdo con la reivindicación 1 o 2, caracterizado porque la interfaz (22) de control está configurada para poner la unidad (23) de control adicional en un estado de reinicio al recibir la señal (31) de error del módulo (30) de supervisión interno y para mantenerlo en el estado de reinicio hasta que finalice la operación de emergencia.
4. Controlador electrónico de potencia programable de acuerdo con cualquiera de las reivindicaciones 1 a 3, caracterizado porque el módulo (20) de control presenta una pluralidad de procesadores, en donde la unidad (21) de control básica y la unidad (23) de control adicional están implementadas cada una en al menos un procesador diferente, o presenta un procesador multinúcleo, en donde la unidad (21) de control básica y la unidad (23) de control adicional están implementadas cada una en al menos un núcleo diferente del procesador multinúcleo.
5. Controlador electrónico de potencia programable de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado porque el módulo (10) de potencia presenta un punto (11) de desconexión del módulo de potencia que está dispuesto entre el módulo (10) de potencia y una conexión al actuador (80) y está configurado para recibir la señal (34) de error del módulo (30) de supervisión interno y, tras su recepción, no transmitir la señal (81) de control del actuador a la conexión al actuador (80).
6. Controlador electrónico de potencia programable de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado porque un transmisor (40) de señales interno, un transmisor (70) de señales externo y/o un módulo (50) de supervisión externo están conectados al módulo (30) de supervisión interno, en donde el transmisor (40) de señales interno, el transmisor (70) de señales externo y/o el módulo (50) de supervisión externo están configurados para enviar señales (41, 51, 71) de datos al módulo (30) de supervisión interno.
7. Controlador electrónico de potencia programable de acuerdo con la reivindicación 6, caracterizado porque el módulo (50) de supervisión externo es un módulo (30) de supervisión interno de otro controlador (200) electrónico de potencia programable.
8. Controlador electrónico de potencia programable de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado porque la unidad (21) de control básica está conectada al módulo (30) de supervisión interno y está configurada para enviar señales (28) de datos al módulo (30) de supervisión interno.
9. Controlador electrónico de potencia programable de acuerdo con cualquiera de las reivindicaciones 6 a 8, caracterizado porque el módulo (30) de supervisión interna está configurado para evaluar las señales (28, 41, 51, 71) de datos recibidas y transmitir una señal (31, 32, 33, 34, 36) de error o una pluralidad de señales (31, 32, 33, 34, 36) de error cuando se detecta una situación de funcionamiento crítica.
10. Controlador electrónico de potencia programable de acuerdo con cualquiera de las reivindicaciones 7 u 8,

caracterizado porque el módulo (30) de supervisión interno está configurado para enviar una señal (32) de error a la unidad (21) de controlador básica, en donde la unidad (21) de control básica está configurada para activar un reinicio de la unidad (21) de control básica al recibir esta señal (32) de error.

5 11. Controlador electrónico de potencia programable de acuerdo con cualquiera de las reivindicaciones 7 a 9, caracterizado porque el módulo (30) de supervisión interno está configurado para enviar una señal (33) de error a la unidad (21) de control básica, en donde la unidad (21) de control básica está configurada para preparar un funcionamiento de emergencia al recibir esta señal (33) de error.

10 12. Controlador electrónico de potencia programable de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado porque solo la unidad (21) de control básica está configurada para emitir señales (29) de control del módulo de potencia al módulo (10) de potencia.

13. Controlador electrónico de potencia programable de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado porque el dispositivo (30) de supervisión interno está configurado para detectar el final del funcionamiento de emergencia y transferir el controlador (200) electrónico de potencia programable del funcionamiento de emergencia al funcionamiento normal.

15 14. Controlador electrónico de potencia programable de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado porque el dispositivo (30) de supervisión interno es una unidad funcional autosuficiente del controlador (200) electrónico de potencia programable, que puede funcionar independientemente del módulo (20) de control.

20 15. Uso de un controlador (200) electrónico de potencia programable de acuerdo con cualquiera de las reivindicaciones 1 a 14, caracterizado porque el controlador (200) de potencia se utiliza para controlar un sistema de paso de una turbina eólica, con el que se fija la posición rotacional de al menos una pala del rotor en un buje del rotor.

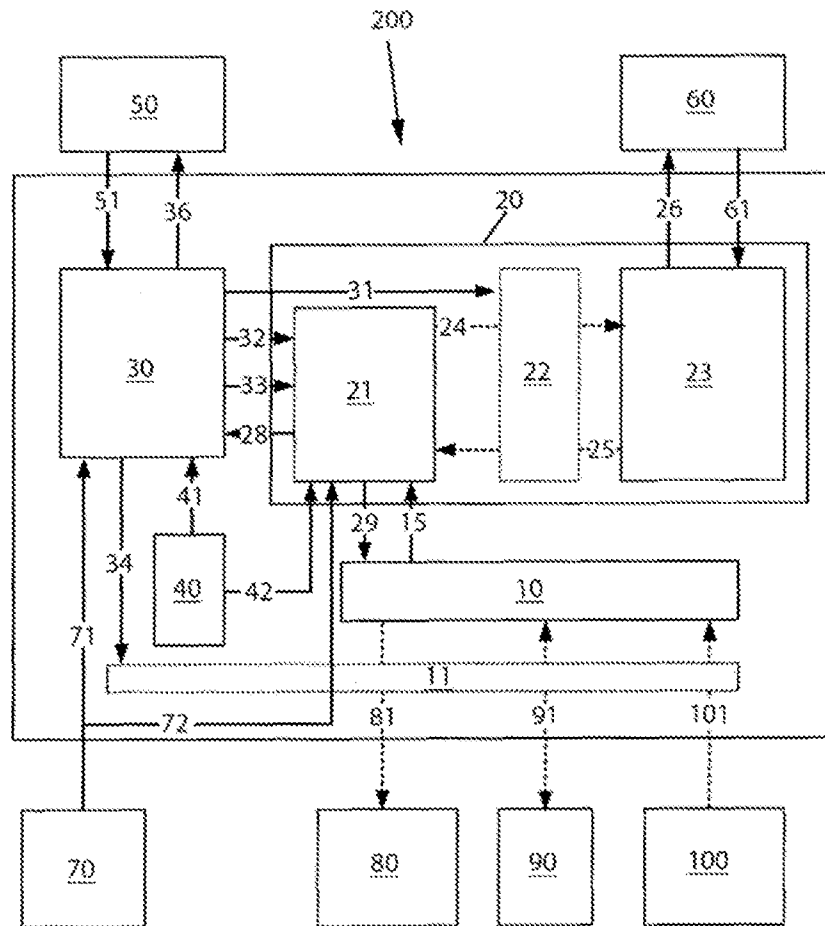


Fig. 1