(19) Deutsches Patent- und Markenamt

(10) **DE 10 2013 213 402 A1** 2015.01.15

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2013 213 402.9**
(22) Anmeldetag: **09.07.2013**
(43) Offenlegungstag: **15.01.2015**

(51) Int Cl.: ***G06F 11/30*** (2006.01)

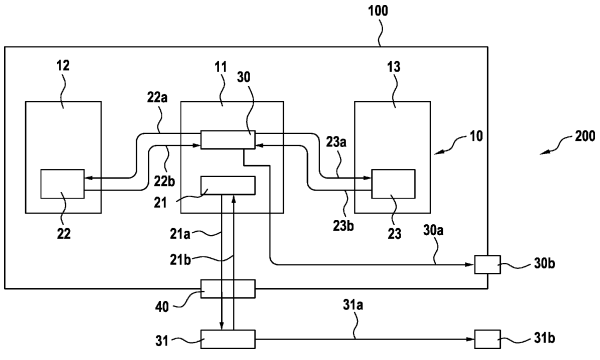
(71) Anmelder:
Robert Bosch GmbH, 70469 Stuttgart, DE

(72) Erfinder:
Dreschmann, Sascha, 71272 Renningen, DE; Rajapakse, Marco, 70378 Stuttgart, DE; Kiewnick, Thomas, 71691 Freiberg, DE; Tatiyosyan, Sevan, 74372 Sersheim, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Mikrocontroller mit mindestens zwei Kernen**

(57) Zusammenfassung: Die Erfindung betrifft einen Mikrocontroller (100) mit mindestens einem ersten Kern (11) und einem zweiten Kern (12), wobei der erste Kern (11) eine interne Überwachungseinheit (30) aufweist und eine erste Sicherheitseinheit (21) aufweist, wobei die erste Sicherheitseinheit (21) eine Schnittstelle (40) aufweist, wobei die Schnittstelle (40) mit einer externen Überwachungseinheit (31) verbindbar ist, wobei der zweite Kern (12) eine zweite Sicherheitseinheit (22) aufweist, wobei die zweite Sicherheitseinheit (22) mit der Überwachungseinheit (30) des ersten Kerns (11) verbunden ist, wobei die interne Überwachungseinheit (30) dazu eingerichtet ist, zu überprüfen, ob der zweite Kern (12) vorbestimmte Sicherheitskriterien erfüllt.



Beschreibung

[0001] Die vorliegende Erfindung betrifft einen Mikrocontroller mit mindestens zwei Kernen, sowie ein Sicherheitssystem zur Fehlersicherung eines Steuergeräts.

Stand der Technik

[0002] Herkömmlicherweise gibt es Sicherheitssteuerungen für technische Anlagen, wie beispielsweise Werkzeugmaschinen, Druckmaschinen, Airbags in Kraftfahrzeugen usw., die durch ein elektrisches, elektronisches und/oder programmierbar elektronisches System gesteuert werden. Ein solches System ist zumeist aus mindestens einer integrierten Schaltung aufgebaut. Der Hauptbestandteil einer solchen integrierten Schaltung ist üblicherweise ein Mikrocontroller, welcher Speicher (z.B. RAM, ROM), einen Zeitgeber bzw. Timer, mindestens einen Mikroprozessor (CPU), einen Eingangsanschluss, einen Ausgangsanschluss und ein die Speicher, den Zeitgeber, die CPU(s), und die Eingangs-/ Ausgangsanschlüsse miteinander verbindendes Bussystem aufweist. Der Mikrocontroller dient zur zentralen Steuerung des elektrischen, elektronischen und/ oder programmierbar elektronischen Systems. Ist die Funktion des Mikrocontrollers aufgrund eines Fehlers, wie beispielsweise Überhitzung oder Überlastung beeinträchtigt, oder fällt der Mikrocontroller aufgrund eines Fehlers sogar ganz aus, ist die Funktion der gesamten zu steuernden technischen Anlage nicht mehr gewährleistet. Daher ist es von erheblicher Bedeutung, einen Ausfall des diese technischen Anlagen steuernden Mikrocontrollers zu vermeiden, bzw. die von dem Mikrocontroller gesteuerte technische Anlage in einen fehlersicheren Betrieb zu überführen.

[0003] Mikrocontroller können mit Mehrkernprozessoren ausgestattet sein, die mehr als einen Prozessorkern aufweisen (sog. Multi-Core-Prozessoren). Dabei können die auszuführenden Funktionen, Anwendungen bzw. Prozesse zweckmäßig auf die einzelnen Kerne des Mikrocontrollers verteilt werden, um beispielsweise freie Rechenleistungen oder Kapazitäten der einzelnen Kerne optimal auszunutzen. Essentielle, sicherheitsrelevante Funktionen können dabei auf sämtliche Kerne des Mikrocontrollers verteilt sein. Jeder der Kerne des Mikrocontrollers muss daher gegen Ausfall und vor Fehlern geschützt sein.

[0004] In der DE 10 2009 015 683 A1 wird ein Sicherheitssystem zur Sicherung eines Mehrkernprozessors beschrieben. Eine externe Überwachungseinrichtung (sog. Watchdog) ist dabei mit den einzelnen Kernen des Mehrkernprozessors verbunden und überwacht diese. Dabei muss eine Schnittstelle zwischen der Überwachungseinrichtung und jedem einzelnen der Kerne des Mehrkernprozessors eingerichtet werden. Die einzelnen Schnittstellen müssen auf Hardware-Basis in die Überwachungseinheit und in den Mehrkernprozessor implementiert werden, was relativ aufwändig ist.

[0005] Es ist wünschenswert, einen Mikrocontroller mit mehreren Kernen bereitzustellen, wobei die einzelnen Kerne des Mikrocontrollers auf einfache, aber sichere Weise gegen Ausfall und Fehler geschützt sind.

Offenbarung der Erfindung

[0006] Erfindungsgemäß werden ein Mikrocontroller mit mindestens zwei Kernen, sowie ein Sicherheitssystem zur Fehlersicherung eines Steuergeräts mit den Merkmalen der unabhängigen Patentansprüche vorgeschlagen. Vorteilhafte Ausgestaltungen sind Gegenstand der Unteransprüche sowie der nachfolgenden Beschreibung.

[0007] In einem erfindungsgemäßen Mikrocontroller weist ein zweiter Kern, insbesondere jeder der einzelnen Kerne des Mikrocontrollers, eine Sicherheitseinheit auf. Eine Überwachungseinheit eines ersten Kerns ist mit der Sicherheitseinheit des zweiten Kerns bzw. insbesondere mit der Sicherheitseinheit eines jeden anderen Kerns des Mikrocontrollers verbunden. Der erste Kern bzw. die Überwachungseinheit des ersten Kerns überwacht somit wenigstens den zweiten Kern und insbesondere alle anderen Kerne des Mikrocontrollers. Die Überwachung der Sicherheitseinheit durch die Überwachungseinheit kann grundsätzlich entsprechend einer Frage-Antwort-Überwachung stattfinden, wie sie beispielsweise in der Veröffentlichung "Standardisiertes E-GAS Überwachungskonzept für Benzin und Diesel Motorsteuerungen. Arbeitskreis EGAS / 16.05.2013 / Version 5.5" als Ebene-3-Überwachung beschrieben wird.

[0008] Es sei darauf hingewiesen, dass zwar in der nachfolgenden Beschreibung zumeist die Rede von zwei Kernen ist. Die Erfindung und ihre Ausführungen sollen allerdings nicht auf zwei Kerne beschränkt sein, sondern können auf beliebig viele Kerne erweitert werden. Insbesondere gelten die nachfolgenden Erläuterungen in Bezug auf den zweiten Kern in analoger Weise für mehrere der Kerne und insbesondere für alle anderen Kerne des Mikrocontrollers.

Vorteile der Erfindung

[0009] Im Zuge der Überprüfung, ob der zweite Kern die vorbestimmten Sicherheitskriterien erfüllt, überprüft die Überwachungseinheit insbesondere, ob der zweite Kern bestimmte Fragen mit einer vorbestimmten Antwort beantwortet. Antwortet der zweite Kern nicht in der vorbestimmten Weise, kann der zweite Kern sicherheitsrelevante Funktionen nicht mehr ent-

sprechend vorbestimmter Sicherheitskriterien ausführen. Die Überwachungseinheit überprüft somit, ob der zweite Kern noch für einen sichereren Betrieb des Mikrocontrollers geeignet ist. Weist der zweite Kern einen Fehler auf oder fällt der zweite Kern aus, wird dies durch die Überwachungseinheit erkannt und die Überwachungseinheit kann entsprechende Maßnahmen ergreifen. Die Überwachungseinheit bzw. der erste Kern sichert den zweiten Kern somit gegen Ausfall ab.

[0010] Durch die erste Sicherheitseinheit bzw. durch die erste Schnittstelle ist der erste Kern mit einer externen Überwachungseinheit (sog. Überwachungsrechner bzw. Watchdog) verbindbar. Unter externer Überwachungseinheit ist dabei zu verstehen, dass die externe Überwachungseinheit kein Teil des Mikrocontrollers ist.

[0011] Der erste Kern kann dabei insbesondere mittels einer externen Überwachungseinheit überwacht werden. Der erste Kern ist demgemäß ein gegen einen Ausfall abgesicherter, überwachter Kern, der wiederum die restlichen Kerne des Mikrocontrollers gegen einen Ausfall absichert und überwacht. Die Schnittstelle zwischen erster Sicherheitseinheit und externer Überwachungseinrichtung kann beispielsweise eine SPI-Schnittstelle sein (Serial Peripheral Interface).

[0012] Um zu überprüfen, ob der zweite Kern die vorbestimmten Sicherheitskriterien erfüllt, können spezielle Algorithmen auf dem ersten und/oder dem zweiten Kern implementiert werden. Diese Algorithmen ermöglichen eine entsprechende Kommunikation zwischen der Überwachungseinheit und der Sicherheitseinheit des zweiten Kerns. Für diese Kommunikation zwischen dem ersten und dem zweiten Kern können insbesondere Kommunikationsschnittstellen genutzt werden, die bereits in dem Mikrocontroller vorhanden sind, beispielsweise ein RAM. Es müssen somit keine zusätzlichen Hardwarebauteile in den Mikrocontroller implementiert werden.

[0013] Dadurch, dass erfindungsgemäß der zweite Kern bzw. sämtliche andere Kerne durch den ersten Kern abgesichert werden, ergeben sich erhebliche Vorteile gegenüber einem Mikrocontroller, in dem alle Kerne mittels einer externen Überwachungseinheit abgesichert sind. Hierzu müsste ein mit der externen Überwachungseinheit verbundener Kern stets auf Daten bzw. eine Rückantwort der anderen Kerne warten, damit er sämtliche Daten bzw. Rückantworten zusammenführen und gemeinsam an die externe Überwachungseinheit übermitteln kann. Dies würde aufgrund von Randbedingungen des Betriebssystems (Jitter von Softwaretasks) zu einer signifikanten Verlängerung einer Fehlerlatenzzeit führen. Zwar könnte die Fehlerlatenzzeit konstant gehalten werden, dies würde allerdings zu einer eingeschränkten Verfügbarkeit des Mikrocontrollers führen.

[0014] Da durch die Erfindung insbesondere jeder der Kerne des Mikrocontrollers überwacht und gegen einen Ausfall abgesichert ist, können auszuführenden Funktionen, Anwendungen und Prozesse beliebig auf die einzelnen Kerne verteilt werden. Es ist nicht notwendig, dass sämtliche sicherheitsrelevante Funktionen auf einem bestimmten Kern ablaufen, der beispielsweise als einziger der Kerne gegen Ausfall abgesichert ist. Die einzelnen Anwendungen und Funktionen können somit zweckmäßig aufgrund von freien Rechenleistungen oder Kapazitäten der einzelnen Kerne verteilt werden.

[0015] Vorzugsweise ist die Überwachungseinheit dazu eingerichtet, den zweiten Kern zu deaktivieren bzw. eine Leistungsendstufe zu deaktivieren, wenn der zweite Kern die vorbestimmten Sicherheitskriterien nicht erfüllt. Die Überwachungseinheit kann dafür insbesondere einen Ausgang aufweisen, über welchen ein spezielles Signal ausgegeben wird, wenn der zweite Kern die vorbestimmten Sicherheitskriterien nicht erfüllt. Des Weiteren können Maßnahmen in die Wege geleitet werden, um den Mikrocontroller in einen sicheren Betriebszustand zu überführen. Beispielsweise können für einen fehlerfreien Betrieb des Mikrocontrollers essentielle Funktionen und Prozesse des zweiten Kerns auf andere Kerne des Mikrocontrollers verteilt werden oder der Mikrocontroller kann in einem speziellen Notfall-Betriebsmodus betrieben oder abgeschaltet werden.

[0016] Vorteilhafterweise ist die Sicherheitseinheit des ersten Kerns über die Schnittstelle mit der externen Überwachungseinheit verbunden. Die externe Überwachungseinheit überwacht somit den ersten Kern auf die gleiche Art, wie der erste Kern den zweiten Kern überwacht. Die externe Überwachungseinheit ist insbesondere als eine Watchdog-Einheit ausgebildet. Dabei kann insbesondere eine herkömmliche Überwachungseinheit bzw. Watchdog-Einheit genutzt werden, die auf herkömmliche Weise dazu eingerichtet ist, eine Komponente zu überwachen. An dieser herkömmlichen Überwachungseinheit bzw. Watchdog-Einheit müssen keinerlei Veränderungen vorgenommen werden. Weder müssen Hardwarebauteile hinzugefügt werden, noch muss dessen Programmierung geändert werden. Es muss keine neue Chipentwicklung der herkömmlichen Überwachungseinheit bzw. Watchdog-Einheit durchgeführt werden und ein bestehendes Design der herkömmlichen Überwachungseinheit bzw. Watchdog-Einheit kann beibehalten werden. Herkömmliche Überwachungseinheiten bzw. Watchdog-Einheiten weisen insbesondere eine einzige Schnittstelle auf, über die sie mit der jeweiligen zu überwachenden Komponente verbunden sind. Dadurch, dass der erfindungsgemäße Mikrocontroller nur eine externe

Schnittstelle in Form der Schnittstelle der ersten Sicherheitseinheit aufweist, ist der erfindungsgemäße Mikrocontroller für die Nutzung mit einer herkömmlichen Überwachungseinheit bzw. Watchdog-Einheit geeignet.

[0017] Bevorzugt ist die externe Überwachungseinheit dazu eingerichtet, den Mikrocontroller zu deaktivieren, wenn der erste Kern die vorgebestimmten Sicherheitskriterien nicht erfüllt. Für diesen Fall, dass der erste Kern einen Fehler aufweist oder ausfällt, kann die Überwachung des zweiten Kerns bzw. der restlichen Kerne nicht mehr von der Überwachungseinheit des ersten Kerns durchgeführt werden.

[0018] In einer vorteilhaften Ausgestaltung der Erfindung weist auch der zweite Kern eine Überwachungseinheit auf, um den ersten Kern zu überwachen. Dadurch können Fehlerlatenzzeiten für alle Kerne reduziert werden, da Parameter der Überprüfung zwischen den einzelnen Kernen leichter zu variieren sind als gegenüber der externen Überwachungseinheit. Fehler oder ein Ausfall eines der Kerne können somit schneller erkannt werden. Die Sicherheitseinheit des ersten Kerns ist dazu mit der Überwachungseinheit des zweiten Kerns und mit der externen Überwachungseinheit verbindbar, entweder über die bereits erwähnte Schnittstelle oder über eine weitere Schnittstelle. Alternativ kann der erste Kern auch zwei Sicherheitseinheiten aufweisen, von denen eine mit der externen Überwachungseinheit verbindbar ist und von denen die andere mit der Überwachungseinheit des zweiten Kerns verbunden ist.

[0019] Bevorzugt führt die Überwachungseinheit des ersten Kerns im Zuge der Überprüfung, ob der zweite Kern die vorbestimmten Sicherheitskriterien erfüllt, eine Frage/Antwort-Kommunikation mit dem zweiten Kern durch. Die Überwachungseinheit stellt dabei Anfragen an die Sicherheitseinheit des zweiten Kerns und diese übermittelt der Überwachungseinheiten Antworten auf diese Anfragen. Auf jede Anfrage existiert eine vorbestimmte Antwort. Die Überwachungseinheit überprüft, ob die Antwort der zweiten Sicherheitseinheit dieser vorbestimmten erwarteten Antwort entspricht. Ist dies nicht der Fall, deutet dies auf einen Fehler bzw. einen Ausfall des zweiten Kerns hin. Vorteilhafterweise wird diese Frage/Antwort Kommunikation mittels eines Program Flow Checks realisiert. Die Überwachungseinheit und die zweite Sicherheitseinheit sind dabei dazu eingerichtet, einen Program Flow Check durchzuführen. Im Zuge dessen bietet es sich insbesondere an, dass die Überwachungseinheit als eine Watchdog-Einheit ausgebildet ist. Analoge Ausführungen gelten für die externe Überwachungseinheit und die erste Sicherheitseinheit bzw. für die zweite Überwachungseinheit und die erste (bzw. vierte) Sicherheitseinheit.

[0020] Die Erfindung betrifft weiterhin ein Sicherheitssystem zur Fehlersicherung eines Steuergeräts mit einem erfindungsgemäßen Mikrocontroller. Ausgestaltungen dieses erfindungsgemäßen Sicherheitssystems ergeben sich aus der obigen Beschreibung des erfindungsgemäßen Mikrocontrollers in analoger Art und Weise.

[0021] Ein erfindungsgemäßer Mikrocontroller bzw. ein erfindungsgemäßes Sicherheitssystem können in vielen Bereichen Anwendung finden und sind insbesondere für Steuergeräte zur Steuerung von technischen Anlagen geeignet, in denen es aus Sicherheitsgründen zum Schutz von Menschenleben oder zur Vermeidung eines großen wirtschaftlichen Schadens notwendig ist, einen Ausfall dieses die technische Anlage steuernden Steuergeräts zu vermeiden bzw. die von dem Steuergerät gesteuerte technische Anlage in einen fehlersicheren Betrieb zu überführen. Derartige technische Anlagen können beispielsweise Werkzeugmaschinen, Druckmaschinen, Kernkraftwerken, Eisenbahnen, Flugzeugen oder Kraftfahrzeugen sein. In Kraftfahrzeugen eignet sich die Erfindung insbesondere für Steuergeräte zur Motorsteuerung und/oder Hybridsteuerung, sowie zur Steuerung von Airbag, ESP, Lenkungssteuergeräte usw.

[0022] Weitere Vorteile und Ausgestaltungen der Erfindung ergeben sich aus der Beschreibung und der beiliegenden Zeichnung.

[0023] Es versteht sich, dass die vorstehend genannten und die nachfolgend noch zu erläuternden Merkmale nicht nur in der jeweils angegebenen Kombination, sondern auch in anderen Kombinationen oder in Alleinstellung verwendbar sind, ohne den Rahmen der vorliegenden Erfindung zu verlassen.

[0024] Die Erfindung ist anhand von Ausführungsbeispielen in der Zeichnung schematisch dargestellt und wird im Folgenden unter Bezugnahme auf die Zeichnung ausführlich beschrieben.

Kurze Beschreibung der Zeichnungen

[0025] **Fig.** 1 zeigt schematisch eine bevorzugte Ausführungsform eines erfindungsgemäßen Mikrocontrollers.

[0026] **Fig.** 2 zeigt schematisch eine weitere bevorzugte Ausführungsform eines erfindungsgemäßen Mikrocontrollers.

Ausführungsform(en) der Erfindung

[0027] In **Fig.** 1 ist eine bevorzugte Ausführungsform eines erfindungsgemäßen Mikrocontrollers schematisch dargestellt und mit **100** bezeichnet. Der Mikro-

controller weist einen Multicore-Prozessor **10** mit drei Kerne **11**, **12** und **13** auf.

[0028] Ein erster Kern **11** weist eine erste Sicherheitseinheit **21** auf, ein zweiter Kern **12** weist eine zweite Sicherheitseinheit **22** auf und ein dritter Kern **13** weist eine dritte Sicherheitseinheit **23** auf. Der erste Kern **11** weist weiterhin eine Überwachungseinheit **30** auf, die sowohl mit der zweiten Sicherheitseinheit **22** des zweiten Kerns **12**, als auch mit der dritten Sicherheitseinheit **23** des dritten Kerns **13** verbunden ist. Mittels einer Schnittstelle **40** ist die erste Sicherheitseinheit **21** mit einer externen Überwachungseinheit **31** verbunden. Die Überwachungseinheit **30** und die externen Überwachungseinheit **31** sind jeweils als eine Watchdog-Einheit ausgebildet.

[0029] Um zu überprüfen, ob der zweite Kern **12** und der dritte Kern **13** vorbestimmte Sicherheitskriterien erfüllen, führt die Überwachungseinheit **30** mit der zweiten Sicherheitseinheit **22** und der dritten Sicherheitseinheit **23** jeweils einen Program Flow Check durch. Die Überwachungseinheit **30** sendet dabei an die zweite Sicherheitseinheit **22** und die dritte Sicherheitseinheit **23** jeweils bestimmte Anfragen, angedeutet durch die Bezugszeichen **22a** und **23a**. Die zweite Sicherheitseinheit **22** und die dritte Sicherheitseinheit **23** senden jeweils Antworten an die Überwachungseinheit **30**, angedeutet durch die Bezugszeichen **22b** und **23b**. Die Überwachungseinheit **30** überprüft, ob die Antworten mit vorbestimmten Antworten übereinstimmen, welche auf die jeweiligen Anfragen erwarteten werden.

[0030] Durch diese Frage/Antwort-Kommunikation **22a**/**22b** bzw. **23a**/**23b** zwischen der Überwachungseinheit **30** und der zweiten Sicherheitseinheit **22** bzw. der dritten Sicherheitseinheit **23** überprüft die Überwachungseinheit **30**, ob der zweite Kern **12** bzw. der dritte Kern **13** jeweils sicherheitsrelevante Funktionen in einem vorbestimmten Zeitintervall ausführt und sicherheitsrelevante Funktionen in einer vorbestimmten Reihenfolge ausführt. Ist dies der Fall, erfüllt der zweite Kern **12** bzw. der dritte Kern **13** die vorbestimmten Sicherheitskriterien.

[0031] Ist dies nicht der Fall, weist der zweite Kern **12** bzw. der dritte Kern **13** einen Fehler auf oder ist ausgefallen. In diesem Fall sendet die Überwachungseinheit **30** ein entsprechendes Signal an einen Ausgang **30b** des Mikrocontrollers, angedeutet durch das Bezugszeichen **30a**. An dem Ausgang **30b** des Mikrocontrollers kann beispielsweise eine Steuereinheit verbunden sein, welche den jeweiligen Kern bzw. eine entsprechende Leistungsendstufe des jeweiligen Kerns deaktiviert, welcher die vorgebestimmten Sicherheitskriterien nicht erfüllt.

[0032] Die Überwachungseinheit **30** bzw. der erste Kern **11** überwacht somit die anderen Kerne **12** und **13** und sichert die anderen Kerne **12** und **13** gegen Ausfall ab. Mittels der externen Überwachungseinheit **31** wird der erste Kern überwacht und gegen Ausfall abgesichert. Diese externe Absicherung ist im Automobilbau beispielsweise als Funktionsrechner/Überwachungsrechner-Absicherung bekannt. Analog zu obiger Beschreibung der Überwachungseinheit **30** führen die externe Überwachungseinheit **31** und die erste Sicherheitseinheit **21** eine Frage/Antwort-Kommunikation in Form eines Program Flow Checks durch. Die externe Überwachungseinheit **31** sendet dabei Anfragen an die erste Sicherheitseinheit **21** des ersten Kerns **11**, angedeutet durch Bezugszeichen **21a**, und die erste Sicherheitseinheit **21** übermittelt entsprechende Antworten an die externe Überwachungseinheit **31**, angedeutet durch Bezugszeichen **21b**. Die externe Überwachungseinheit **31** überprüft, ob diese Antworten erwarteten vorbestimmten Antworten entsprechen und überprüft somit, ob der erste Kern die vorbestimmten Sicherheitskriterien erfüllt.

[0033] Ist dies nicht der Fall, sendet die externe Überwachungseinheit **31** ein entsprechendes Signal an einen Ausgang **31b**, angedeutet durch das Bezugszeichen **31a**. An dem Ausgang **31b** kann ebenfalls eine Steuereinheit verbunden sein, welche den Mikrocontroller eine entsprechende Leistungsendstufe des Mikrocontrollers deaktiviert, wenn der erste Kern **11** die vorgebestimmten Sicherheitskriterien nicht erfüllt.

[0034] Der Mikrocontroller **100** und die externen Überwachungseinheit **31** bilden eine bevorzugte Ausgestaltung einer erfindungsgemäßen Sicherheitssystem **200** und sind Teil eines Steuergeräts, beispielsweise eines Steuergeräts eines Kraftfahrzeugs.

[0035] In **Fig.** 2 ist eine weitere bevorzugte Ausführungsform eines erfindungsgemäßen Mikrocontrollers **100** bzw. eines erfindungsgemäßen Sicherheitssystems **200** schematisch dargestellt. Identische Bezugszeichen beziehen sich dabei auf identische Teile der **Fig.** 1.

[0036] Dabei weist der zweite Kern **12** eine zweite Überwachungseinheit **32** auf. Des Weiteren weist der erste Kern **11** zusätzlich zu der ersten Sicherheitseinheit eine vierte Sicherheitseinheit **24** auf. Die zweite Überwachungseinheit **32** ist mit der vierten Sicherheitseinheit **24** verbunden. Analog zu obiger Beschreibung überprüft die zweite Überwachungseinheit **32**, ob der erste Kern **11** die vorbestimmten Sicherheitskriterien erfüllt. Dazu sendet die zweite Überwachungseinheit **32** Anfragen an die vierten Sicherheitseinheit **24**, angedeutet durch Bezugszeichen **24a**, und erhält von dieser Antworten, angedeutet durch Bezugszeichen **24b**. Erfüllt der erste Kern **11** die vorbestimmten Sicherheitskriterien nicht, sendet die zweite Überwachungseinheit **32** ein ent-

sprechendes Signal an einen Ausgang **32b** des Mikrocontrollers **100**, angedeutet durch das Bezugszeichen **32a**. Analog zu obiger Beschreibung kann an dem Ausgang **32b** eine Steuereinheit verbunden sein, welche den Mikrocontroller bzw. eine entsprechende Leistungsendstufe des Mikrocontrollers deaktiviert, wenn der erste Kern **11** die vorgebestimmten Sicherheitskriterien nicht erfüllt.

[0037] Der erste Kern **11** kann zusätzlich weiterhin über die erste Sicherheitseinheit **21** mit der externen Überwachungseinheit **31** verbunden sein und zusätzlich von dieser überwacht und gegen Ausfall gesichert sein.

[0038] Alternativ kann der erste Kern **11** auch über die erste Sicherheitseinheit **21** mit der zweiten Überwachungseinheit **32** verbunden sein und keine vierte Sicherheitseinheit **24** aufweisen. Dabei kann die erste Sicherheitseinheit **21** entweder mit der zweiten Überwachungseinheit **32** oder der externen Überwachungseinheit **31** verbindbar sein, oder mit der zweiten Überwachungseinheit **32** und der externen Überwachungseinheit **32** gleichzeitig.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- DE 102009015683 A1 [0004]

Patentansprüche

1. Mikrocontroller (**100**) mit mindestens einem ersten Kern (**11**) und einem zweiten Kern (**12**), wobei
– der erste Kern (**11**)
– eine interne Überwachungseinheit (**30**) aufweist und
– eine erste Sicherheitseinheit (**21**) aufweist, wobei die erste Sicherheitseinheit (**21**) eine Schnittstelle (**40**) aufweist, wobei die Schnittstelle (**40**) mit einer externen Überwachungseinheit (**31**) verbindbar ist,
– der zweite Kern (**12**) eine zweite Sicherheitseinheit (**22**) aufweist, wobei die zweite Sicherheitseinheit (**22**) mit der Überwachungseinheit (**30**) des ersten Kerns (**11**) verbunden ist,
– wobei die interne Überwachungseinheit (**30**) dazu eingerichtet ist, zu überprüfen, ob der zweite Kern (**12**) vorbestimmte Sicherheitskriterien erfüllt.

2. Mikrocontroller (**100**) nach Anspruch 1, wobei die interne Überwachungseinheit (**30**) dazu eingerichtet ist den zweiten Kern (**12**) oder den Mikrocontroller (**100**) zu deaktivieren, wenn der zweite Kern (**12**) die vorbestimmten Sicherheitskriterien nicht erfüllt.

3. Mikrocontroller (**100**) nach einem der vorstehenden Ansprüche, wobei der zweite Kern (**12**) eine zweite Überwachungseinheit (**32**) aufweist, wobei die erste Sicherheitseinheit (**21**) mit der zweiten Überwachungseinheit (**32**) verbundent ist.

4. Mikrocontroller (**100**) nach Anspruch 3, wobei die erste Sicherheitseinheit (**21**) mit der zweiten Überwachungseinheit (**32**) verbunden ist und die zweite Überwachungseinheit (**32**) dazu eingerichtet ist, über die erste Sicherheitseinheit (**21**) zu überprüfen, ob der erste Kern (**11**) die vorbestimmten Sicherheitskriterien erfüllt.

5. Mikrocontroller (**100**) nach einem der vorstehenden Ansprüche, wobei die interne Überwachungseinheit (**30**) dazu eingerichtet ist, im Zuge der Überprüfung, ob der zweite Kern (**12**) die vorbestimmten Sicherheitskriterien erfüllt, Anfragen an die zweite Sicherheitseinheit (**22**) zu stellen (**22a**) und zu überprüfen, ob Antworten der zweiten Sicherheitseinheit (**12**) auf die Anfragen erwarteten Antworten entsprechen.

6. Mikrocontroller (**100**) nach einem der vorstehenden Ansprüche, wobei die interne Überwachungseinheit (**30**) und die zweite Sicherheitseinheit (**22**) dazu eingerichtet sind, im Zuge der Überprüfung, ob der zweite Kern (**12**) die vorbestimmten Sicherheitskriterien erfüllt, einen Program Flow Check durchzuführen.

7. Sicherheitssystem (**200**) zur Fehlersicherung eines Steuergeräts, aufweisend einen Mikrocontroller (**100**) nach einem der vorstehenden Ansprüche und eine externe Überwachungseinheit (**31**), die über die Schnittstelle (**40**) mit der ersten Sicherheitseinheit (**21**) des ersten Kerns (**11**) des Mikrocontrollers (**100**) verbunden ist, wobei die externe Überwachungseinheit (**31**) dazu eingerichtet ist, über die erste Sicherheitseinheit (**21**) zu überprüfen, ob der erste Kern (**21**) die vorbestimmten Sicherheitskriterien erfüllt.

8. Sicherheitssystem (**200**) nach Anspruch 7, wobei die externe Überwachungseinheit (**31**) dazu eingerichtet ist, den ersten Kern (**11**) oder den Mikrocontroller (**100**) zu deaktivieren, wenn der erste Kern (**11**) die vorbestimmten Sicherheitskriterien nicht erfüllt.

Es folgen 2 Seiten Zeichnungen

Anhängende Zeichnungen

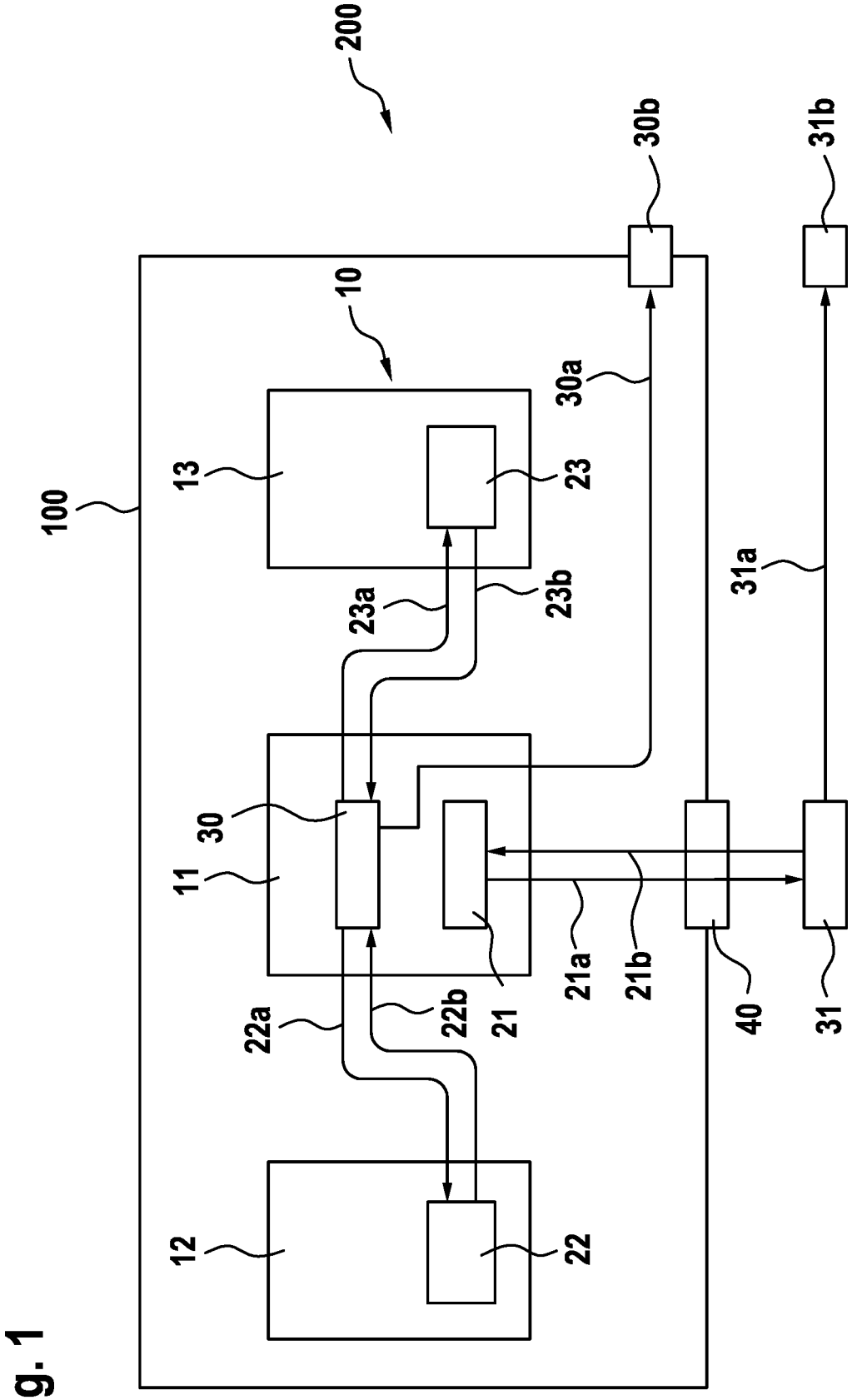


Fig. 1

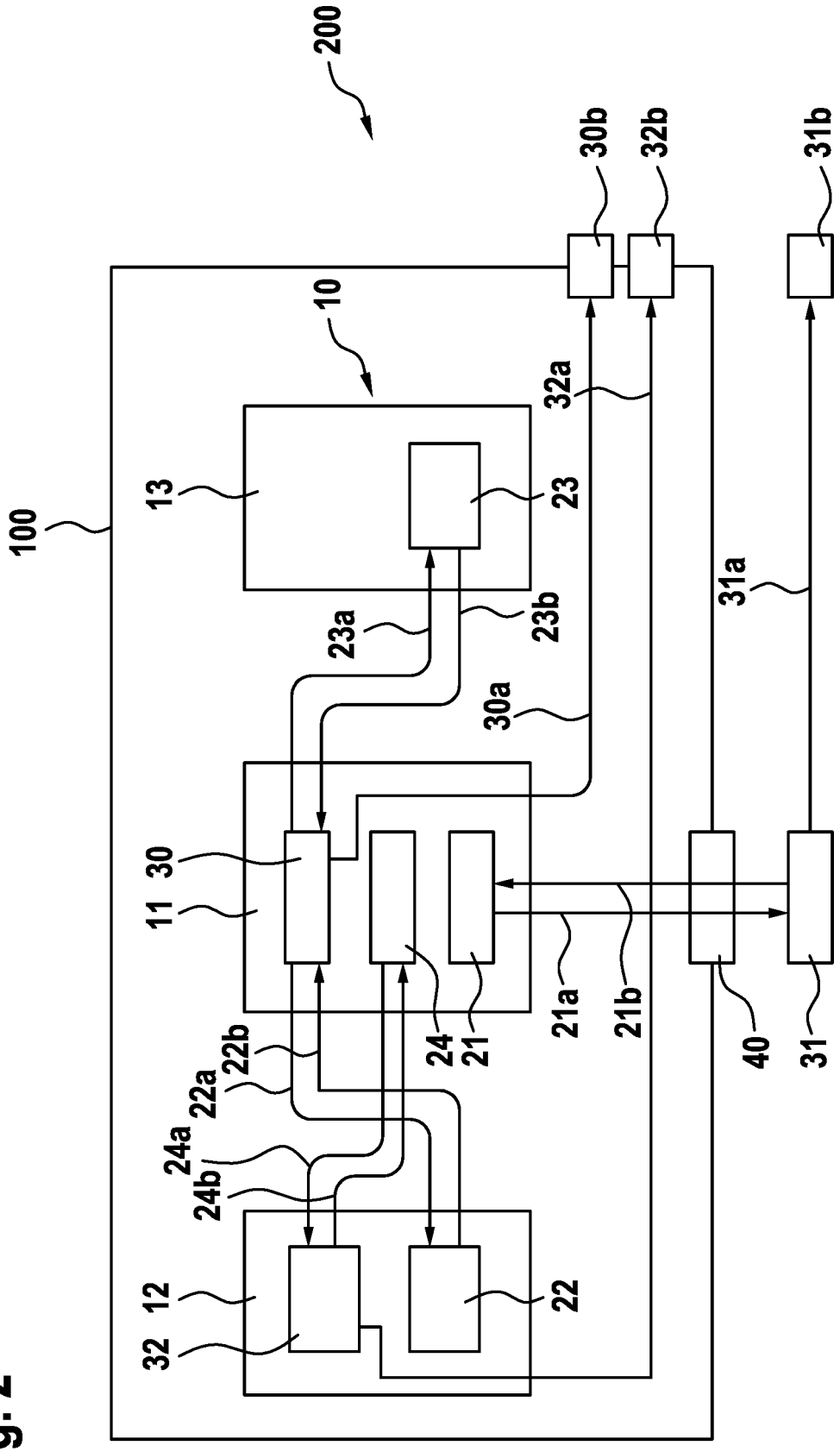

200
30b
32b
31b
10
32a
13
23
100
31a
23a
23b
30a
30
11
21a
21b
24
21
40
31
22b
22a
24a
24b
12
22
32

Fig. 2