(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 139 354 A2**

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
08.03.2017 Patentblatt 2017/10

(51) Int Cl.:
G07C 9/00 *(2006.01)*

(21) Anmeldenummer: **16183331.4**

(22) Anmeldetag: **09.08.2016**

(84) Benannte Vertragsstaaten:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Benannte Erstreckungsstaaten:
BA ME
Benannte Validierungsstaaten:
MA MD

(30) Priorität: **03.09.2015 DE 102015114717**

(71) Anmelder: **EUCHNER GmbH + Co. KG**
70771 Leinfelden-Echterdingen (DE)

(72) Erfinder: **Rothenburg, Jens**
72622 Nürtingen (DE)

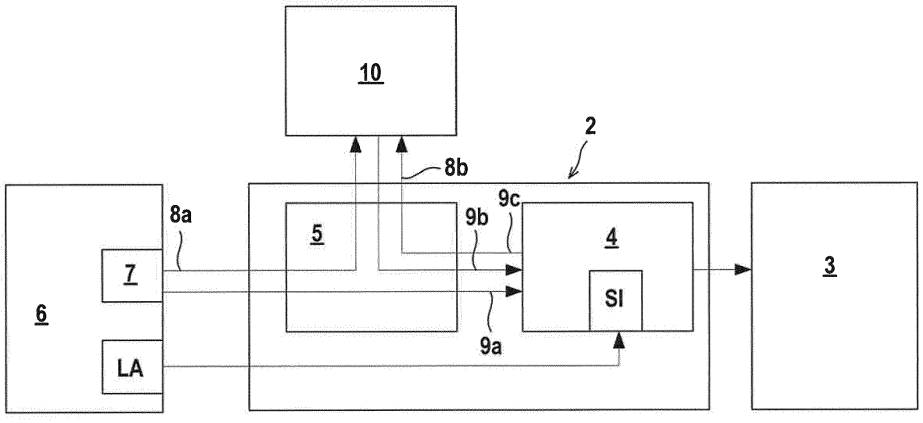
(74) Vertreter: **Ruckh, Rainer Gerhard**
Patentanwalt
Jurastrasse 1
73087 Bad Boll (DE)

(54) **VERFAHREN ZUR EINSTELLUNG EINER BETRIEBSART EINES SICHERHEITSSYSTEMS**

(57) Die Erfindung betrifft ein Verfahren zur Einstellung einer Betriebsart eines Sicherheitssystems (1), umfassend ein Zugangssystem, welches an ein eine Maschine steuerndes Steuerungssystem (2) angeschlossen ist. Das Steuerungssystem (2) weist eine Sicherheitssteuerung (4) auf. Das Verfahren umfasst folgende Verfahrensschritte:

• Zweikanaliges Auslesen von Signalen des Zugangssystems in das Steuerungssystem (1)
• Durchführen einer Gültigkeitsüberprüfung der Signale des Zugangssystems in dem Steuerungssystem (2)
• wobei das Steuerungssystem (2) nur bei Vorliegen gültiger Signale des Zugangssystems die Auswahl einer Betriebsart über die Eingabeeinheit (10) freigibt.
• Durchführen einer Fehlerkontrolle der Auswahl der Betriebsart in der Sicherheitssteuerung (4)
• Umschalten auf die ausgewählte Betriebsart durch die Sicherheitssteuerung (4) nach positiv durchgeführter Fehlerkontrolle.

Fig. 1



EP 3 139 354 A2

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Einstellung einer Betriebsart eines Sicherheitssystems sowie ein Sicherheitssystem zur Durchführung des Verfahrens.

[0002] Ein derartiges Sicherheitssystem umfasst generell ein Steuerungssystem, das eine Maschine steuert. Von der Maschine können Gefahren für Personen ausgehen. Als Sicherheitsmaßnahme wird daher ein Gefahrenbereich an der Maschine überwacht. Ein wesentliches Sicherheitselement bildet hierbei ein an das Steuerungssystem angeschlossenes Zugangssystem, mittels dessen ein kontrollierter Zugang zu sicherheitsrelevanten Steuerungsfunktionen überwacht wird. Ein derartiges Zugangssystem kann beispielsweise von einem elektronischen Schlüsselsystem gebildet sein. Dieses elektronische Schlüsselsystem umfasst einen Schlüsseleinsatz und wenigstens einen diesem zugeordneten Schlüssel. Der Schlüssel umfasst typischerweise einen Transponder, in dem ein Code enthalten ist. Im Schlüsseleinsatz ist eine Erkennungseinrichtung integriert, mittels derer berührungslos der Code im Schlüssel dann ausgelesen werden kann, wenn der Schlüssel in einer Eingriffsstellung im Schlüsseleinsatz ist. Der Code des Schlüssels kann ein Steuerungssignal für das Starten oder Stoppen der Maschine enthalten. Weiterhin kann der Code Berechtigungsdaten oder prozessorientierte Informationen wie Parameter für den Betrieb der Maschine enthalten.

[0003] Typischerweise ist der Gefahrenbereich der Maschine mit einer Schutzabdeckung oder Umzäunung gesichert. In der Umzäunung befindet sich dann eine Schutztür. Abhängig davon ob die Schutztür geschlossen ist oder nicht kann mit der Maschine in unterschiedlichen Betriebsarten gearbeitet werden.

[0004] Bei derartigen Sicherheitssystemen sind generell mehrere Betriebsarten möglich. Eine erste Betriebsart ist der Automatikbetrieb. In diesem Sicherheitsbetrieb darf sich keine Person im Gefahrenbereich befinden und die Schutztür ist geschlossen. In diesem Automatikbetrieb ist der Arbeitsbetrieb der Maschine uneingeschränkt freigegeben, so dass mit dieser insbesondere auch Arbeitsvorgänge durchgeführt werden, die zu Gefährdungen von Personen im Gefahrenbereich führen könnten. Zusätzlich sind weitere Betriebsarten möglich, bei welchen die Sicherheitsüberwachung überbrückt ist. Bei derartigen Betriebsarten kann beispielsweise durch entsprechende Codierungen von Schlüsseln befugten Personen Zugang zum Gefahrenbereich gewährt werden, beispielsweise um dort Reparatur- oder Installationsarbeiten durchzuführen. Je nach Betriebsart kann dann die Maschine komplett angehalten oder in einem eingeschränkten Betriebsmodus, beispielsweise mit reduzierter Geschwindigkeit, gefahren werden.

[0005] Ein Problem bei derartigen Sicherheitssystemen besteht darin, dass eine Umschaltung der Betriebsart aufgrund gesetzlicher Bestimmungen auf befugte Personen beschränkt werden muss. Zudem ist für die Umschaltung ein Sicherheitsniveau gefordert, dass nicht mit beliebigen konventionellen Systemen erreicht werden kann sondern den Einsatz von Sicherheitstechnik notwendig macht.

[0006] Bei einer ersten bekannten Betriebsartumschaltung wird die jeweilige Betriebsart über einen oder mehrere Schlüsselschalter an der Maschine ausgewählt. Nachteilig hierbei ist, dass die Schlüssel leicht kopiert werden können und die Kontrolle über den Zugang nicht gewährleistet ist.

[0007] Bei einer zweiten bekannten Betriebsartumschaltung sind an der Maschine Tasten vorgesehen, die mittels eines Schlüssels freigeschaltet werden können. Auch diese Lösung hat die genannten Nachteile.

[0008] Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren und ein Sicherheitssystem bereitzustellen, mittels dessen bei geringem konstruktivem Aufwand eine sichere Betriebsarteinstellung ermöglicht wird.

[0009] Zur Lösung dieser Aufgabe sind die Merkmale der unabhängigen Ansprüche vorgesehen. Vorteilhafte Ausführungsformen und zweckmäßige Weiterbildungen der Erfindung sind in den abhängigen Ansprüchen beschrieben.

[0010] Die Erfindung betrifft ein Verfahren zur Einstellung einer Betriebsart eines Sicherheitssystems, umfassend ein Zugangssystem, welches an ein eine Maschine steuerndes Steuerungssystem angeschlossen ist. Das Steuerungssystem weist eine Sicherheitssteuerung auf. Das Verfahren umfasst folgende Verfahrensschritte:

- Zweikanaliges Auslesen von Signalen des Zugangssystems in das Steuerungssystem,
- Durchführen einer Gültigkeitsüberprüfung der Signale des Zugangssystems in dem Steuerungssystem,
- wobei das Steuerungssystem nur bei Vorliegen gültiger Signale des Zugangssystems die Auswahl einer Betriebsart über die Eingabeeinheit freigibt,
- Durchführen einer Fehlerkontrolle der Auswahl der Betriebsart in der Sicherheitssteuerung,
- Umschalten auf die ausgewählte Betriebsart durch die Sicherheitssteuerung nach positiv durchgeführter Fehlerkontrolle.

[0011] Weiterhin betrifft die Erfindung ein Sicherheitssystem zur Durchführung des erfindungsgemäßen Verfahrens.

[0012] Ein wesentlicher Vorteil des erfindungsgemäßen Verfahrens beziehungsweise des erfindungsgemäßen Sicherheitssystems besteht darin, dass ohne konstruktiven Zusatzaufwand eine fehlersichere Einstellung der Betriebsart des Sicherheitssystems beziehungsweise der damit gesicherten Maschine ermöglicht wird.

[0013] Für diese Betriebsarteinstellung können bereits

am Sicherheitssystem standardmäßig vorhandene Komponenten genutzt werden. Dies gilt insbesondere für die Eingabeeinheit, die vorteilhaft in Form eines Touchscreens oder mittels sogenannten Softkeys ausgebildet ist.

[0014] Die fehlersichere Auswahl und Einstellung einer Betriebsart wird insbesondere durch Fehlerkontrollen des Steuerungssystems gewährleistet, wobei diese als wesentliche Komponente eine Sicherheitssteuerung und besonders vorteilhaft eine nichtfehlersichere Steuerung aufweist.

[0015] Durch diese Fehlerkontrollen werden die Komponenten des Sicherheitssystems getestet und eventuelle Fehler aufgedeckt. Vorteilhaft hierbei ist, dass bei den Fehlerkontrollen in den einzelnen Komponenten, insbesondere der Eingabeeinheit, der nichtfehlersicheren Steuerung und Sicherheitssteuerung, synchrone Abläufe vorgesehen sind, wodurch parallele Kanäle erhalten werden, durch deren Vergleich mit hoher Sicherheit auftretende Fehler aufgedeckt werden können, und zwar im gesamten Sicherheitssystem, da bei den Fehlerkontrollen alle Komponenten des Sicherheitssystems umfasst sind.

[0016] Ein wesentlicher Aspekt der Erfindung besteht darin, dass das Zugangssystem eine zweikanalige, vorzugsweise diversitäre Ausgangsstruktur aufweist, so dass von dem Zugangssystem zweikanalig Signale in das Steuerungssystem eingelesen werden. Durch die Auswertung der Signale kann über die Sicherheitssteuerung kontrolliert werden, ob das Steuerungssystem, insbesondere die nichtfehlersichere Steuerung, sowie das Zugangssystem korrekt arbeiten.

[0017] Besonders vorteilhaft werden hierzu die Signale wenigstens eines Ausgangs des Zugangssystems in der Sicherheitssteuerung für eine Gültigkeitsüberprüfung herangezogen.

[0018] Weiter vorteilhaft werden Signale eines Ausgangskanals des Zugangssystems in der nichtfehlersicheren Steuerung ausgewertet, insbesondere derart, ob die Signale des Ausgangskanals gültig sind, was beispielsweise anhand einer Prüfsummenberechnung der Signale erfolgen kann. Die über den zweiten Ausgangskanal in die Sicherheitssteuerung eingelesenen Signale werden dann vorteilhaft für eine Zeitüberwachung derart genutzt, indem geprüft wird, ob die Signale des ersten Ausgangssignals in einem vorgegebenen Zeitfenster eingelesen werden. Durch diese diversitäre zweikanalige Überwachungsstruktur wird eine hohe Fehlersicherheit erreicht.

[0019] Gemäß einer besonders vorteilhaften Ausführungsform der Erfindung ist das Zugangssystem von einem elektronischen Schlüsselsystem, umfassend einen Schlüsseleinsatz und wenigstens einen Schlüssel, gebildet. Das Zugangssystem weist einen Datenausgang auf, über welchen Daten eines im Schlüsseleinsatz befindlichen Schlüssels in die nichtfehlersichere Steuerung eingelesen werden. Das Zugangssystem weist einen Schaltausgang auf, über welchen ein Schaltsignal, dessen Schaltzustände angeben, ob ein Schlüssel im Schlüsseleinsatz vorhanden ist oder nicht, in die Sicherheitssteuerung eingelesen wird.

[0020] Dies stellt eine besonders zweckmäßige Ausgestaltung einer diversitären zweikanaligen Ausgangsstruktur dar. Die nichtfehlersichere Steuerung, die keinen fehlersicheren Aufbau aufweist, ist gut geeignet, größere Datenmengen wie die vom Schlüssel eingelesenen Daten zu verarbeiten. Die Sicherheitssteuerung mit ihrem fehlersicheren Aufbau muss demgegenüber nur eine erheblich reduzierte Datenmenge verarbeiten, da das über den Schaltausgang des Zugangssystems eingelesene Schaltsignal ein binäres Signal ist. Soweit die Sicherheitssteuerung weitere Daten des Zugangssystems von der nichtfehlersicheren Steuerung zur Durchführung von Fehlerkontrollen benötigt, so werden diese in ein von der Sicherheitssteuerung verarbeitbares Format gewandelt. Generell werden dabei nur die für die Fehlerkontrolle erforderlichen Daten an die Sicherheitssteuerung gesendet, so dass die Datenmenge geringen gehalten werden kann. Somit ergibt sich eine zweckmäßige Arbeitsteilung für das Steuerungssystem derart, dass die nichtfehlersichere Steuerung zum Bearbeiten größerer Datenmengen genutzt wird, während in der Sicherheitssteuerung nur geringe Datenmengen verarbeitet werden müssen, so dass die Funktion der Sicherheitssteuerung auf die durchzuführenden Fehlerkontrollen begrenzt werden kann.

[0021] Gemäß einer besonders vorteilhaften Ausführungsform der Erfindung wird als erste Gültigkeitsüberprüfung von Signalen des Zugangssystems bei Einlesen eines Schaltsignals, dessen Schaltzustand einen im Schlüsseleinsatz befindlichen Schlüssel signalisiert, in der Sicherheitssteuerung eine Zeiterwartung durch Öffnen eines Zeitintervalls gestartet. In der Sicherheitssteuerung wird geprüft, ob innerhalb dieses Zeitintervalls Daten des Schlüssels über den Datenausgang in die nichtfehlersichere Steuerung eingelesen wurden. Als zweite Gültigkeitsüberprüfung wird eine Prüfsummenberechnung der vom Datenausgang eingelesenen Daten des Schlüssels in der nichtfehlersicheren Steuerung durchgeführt.

[0022] Bei dieser Ausführungsform wird eine zweikanalige Überprüfungsstruktur realisiert, da Fehlerkontrollen nicht nur in der Sicherheitssteuerung, sondern auch in der nichtfehlersicheren Steuerung durchgeführt werden. Durch den synchronen Ablauf der Fehlerkontrollen und deren gegenseitige Kontrollen wird eine umfangreiche Testung des Steuerungssystems und des Zugangssystems realisiert.

[0023] Besonders vorteilhaft sendet die nichtfehlersichere Steuerung nach erfolgreicher Gültigkeitsüberprüfung ein Autorisierungssignal an die Eingabeeinheit, wodurch Eingaben an der Eingabeeinheit freigegeben werden.

[0024] Dies stellt eine zweckmäßige Arbeitsteilung innerhalb des Gesamtsystems deshalb dar, da die nichtfehlersichere Steuerung als zur Verarbeitung größerer

Datenmengen ausgebildete Einheit den Datenverkehr mit der Eingabeeinheit übernimmt.

[0025] Besonders vorteilhaft ist die Eingabeeinheit von einem Touchscreen oder durch sogenannte Softkeys gebildet.

[0026] Dies stellt eine besonders komfortable, einfach bedienbare Oberfläche für einen Benutzer des Sicherheitssystems dar.

[0027] Obwohl die Eingabeeinheit und die zu deren Ansteuerung verwendete nichtfehlersichere Steuerung selbst keinen fehlersicheren Aufbau aufweisen, wird über diese Struktur eine fehlersichere Betriebsartauswahl gewährleistet. Dies beruht darauf, dass nicht nur die nichtfehlersichere Steuerung, sondern auch die Eingabeeinheit in das Gesamtsystem der Fehlerkontrolle integriert ist.

[0028] Eine erste Fehlerkontrolle besteht darin, dass eine Freigabe der Eingabeeinheit zur Durchführung von Eingaben durch einen Nutzer erst dann erfolgt, wenn in dem Steuerungssystem, insbesondere der nichtfehlersicheren Steuerung, die Gültigkeitsüberprüfung der vom Datenausgang des Zugangssystems durchgeführten Prüfsummenberechnung erfolgreich war und damit einfache Fehler auf dem nicht sicheren elektronischem Schlüssel erkannt werden können sowie ein Schutz gegen das Kopieren eines Schlüssels realisiert ist.

[0029] Weiterhin wird in der nichtfehlersicheren Steuerung als Fehlerkontrolle geprüft, ob die ausgewählte Betriebsart in einem zulässigen Bereich liegt.

[0030] Damit wird vom fehlersicheren Teil des Steuerungssystems direkt die Funktion der Eingabeeinheit geprüft. Zweckmäßigerweise ist in der Sicherheitssteuerung hierzu eine Liste zulässiger Eingaben hinterlegt. Diese Liste kann gegebenenfalls mit den vom Zugangssystem eingelesenen Daten abgeglichen werden, beispielsweise derart, dass je nach in den Daten enthaltener Zugriffsberechtigung nur noch eine Teilmenge der in der Sicherheitssteuerung hinterlegten Betriebsarten als von der Eingabeeinheit auswählbar markiert wird.

[0031] Weiterhin wird zur Fehlerkontrolle einer ausgewählten Betriebsart diese auf die Eingabeeinheit rückgelesen.

[0032] Durch dieses Rücklesen wird einerseits dem Benutzer die Möglichkeit gegeben, zu prüfen, ob seine Eingabe korrekt war, beziehungsweise korrekt verarbeitet wurde. Weiterhin erfolgt durch das Überprüfen des Rücklesens in der Sicherheitssteuerung eine weitere Fehlerkontrolle der Eingabeeinheit und der diese steuerenden nichtfehlersicheren Steuerung.

[0033] Schließlich wird bei Aufdeckung eines Fehlers in dem Steuerungssystem eine Fehlerverrastung erzeugt.

[0034] Damit ist das Konzept der Fehlerkontrolle zur Gewährleistung einer sicheren Auswahl und einer sicheren Einstellung einer Betriebsart bei dem erfindungsgemäßen Sicherheitssystem komplettiert. Wesentlich ist, dass unabhängig davon, wo und an welcher Stelle des Sicherheitssystems ein Fehler aufgedeckt wird, sofort eine Fehlerverrastung erfolgt und das Gesamtsystem somit in einen sicheren Zustand übergeht. Dabei ist weiterhin wesentlich, dass im Sicherheitssystem bei Auftreten eines Fehlers nicht nur eine Fehlermeldung erfolgt, sondern eine Fehlerverrastung. Fehlerverrastung in diesem Zusammenhang bedeutet, dass bei Auftreten eines Fehlers die Prozedur für eine Betriebsartauswahl gestoppt wird, bis eine spezifische, applikationsspezifisch vorgebbare Aktion durchgeführt wurde, welche die Fehlerverrastung aufhebt.

[0035] Die Erfindung wird im Folgenden anhand der Zeichnungen erläutert. Es zeigen:

Figur 1: Schematische Darstellung eines Ausführungsbeispiels des erfindungsgemäßen Sicherheitssystems.

Figur 2a-f: Ablaufdiagramm zur fehlersicheren Einstellung einer Betriebsart des Sicherheitssystems gemäß Figur 1.

[0036] Figur 1 zeigt schematisch den Aufbau eines Ausführungsbeispiels des erfindungsgemäßen Sicherheitssystems 1. Das Sicherheitssystem 1 umfasst ein Steuerungssystem 2, das den Betrieb einer Maschine 3 steuert. Das Steuerungssystem 2 umfasst dabei eine Sicherheitssteuerung 4, die von einer fehlersicheren SPS-Steuerung gebildet sein kann. Weiterhin umfasst das Steuerungssystem 2 eine nichtfehlersichere Steuerung 5, die von einer nichtfehlersicheren SPS-Steuerung gebildet ist.

[0037] Mit der vom Steuerungssystem 2 gesteuerten Maschine 3 werden Arbeitsprozesse durchgeführt, die innerhalb eines Gefahrenbereichs um die Maschine 3 zu Gefährdungen von Personen führen können. Zur Absicherung des Gefahrenbereichs ist dieser mit einer nicht dargestellten Umzäunung oder Umhausung abgegrenzt. In der Umzäunung befindet sich eine ebenfalls nicht dargestellte Schutztür, über welche Personen Zugang zum Gefahrenbereich erhalten können.

[0038] Der Zugang zur Auswahl einer Betriebsart wird mittels eines Zugangssystems überwacht, welches im vorliegenden Fall von einem elektronischen Schlüsselsystem 6 gebildet ist. Dieses elektronische Schlüsselsystem 6 umfasst einen nicht dargestellten Schlüsseleinsatz und wenigstens einen diesem zugeordneten, ebenfalls nicht dargestellten Schlüssel. Der Schlüssel umfasst typischerweise einen Transponder, in dem ein Code enthalten ist. Im Schlüsseleinsatz ist eine Erkennungseinrichtung integriert, mittels derer berührungslos der Code im Schlüssel dann ausgelesen werden kann, wenn der Schlüssel in einer Eingriffsstellung im Schlüsseleinsatz ist. Der Code des Schlüssels kann Berechtigungsdaten sowie weitere prozessorientierte Informationen wie Parameter für den Betrieb der Maschine 3 enthalten.

[0039] Das elektronische Schlüsselsystem 6 weist, wie in Figur 1 dargestellt, eine diversitäre, zweikanalige Ausgangsstruktur auf. Diese umfasst einen Datenausgang

7, über welchen Daten des im Schlüsseleinsatz befindlichen Schlüssels ausgelesen werden können. Weiterhin ist ein Schaltausgang LA vorgesehen, über welchen ein binäres Schaltsignal ausgelesen werden kann. Die Schaltzustände des Schaltsignals geben an, ob ein Schlüssel in Eingriff mit dem Schlüsseleinsatz ist oder nicht. Wie aus Figur 1 ersichtlich, wird das Schaltsignal des elektronischen Schlüsselsystems 6 über einen Schalteingang SI in die Sicherheitssteuerung 4 eingelesen. Die Daten des Datenausgangs 7 werden dagegen über Busleitungen 8a eines Bussystems in die nichtfehlersichere Steuerung 5 eingelesen. Wie Figur 1 weiter zeigt, findet zwischen der Sicherheitssteuerung 4 und der nichtfehlersicheren Steuerung 5 über Leitungen 9a, 9b, 9c ein bidirektionaler Datenaustausch statt. Schließlich ist über Busleitungen 8b des Bussystems eine Eingabeeinheit 10 an die nichtfehlersichere Steuerung 5 angeschlossen und wird von dieser gesteuert.

[0040] Die Eingabeeinheit 10 ist im vorliegenden Fall von einem Touchscreen gebildet. Über den Touchscreen können für den Betrieb des Sicherheitssystems 1 relevante Informationen eingegeben werden.

[0041] Das Sicherheitssystem 1 gemäß Figur 1 kann in mehreren Betriebsarten betrieben werden. Eine erste Betriebsart ist der Automatikbetrieb. In diesem Automatikbetrieb darf sich keine Person im Gefahrenbereich befinden und die Schutztür ist geschlossen, so dass ein Eindringen von Personen in den Gefahren verhindert ist. In diesem Automatikbetrieb ist der Arbeitsbetrieb der Maschine 3 uneingeschränkt freigegeben, so dass mit dieser insbesondere auch Arbeitsvorgänge durchgeführt werden, die zu Gefährdungen von Personen im Gefahrenbereich führen könnten. Zusätzlich sind weitere Betriebsarten möglich, bei welchen die Sicherheitsüberwachung überbrückt ist. Bei derartigen Betriebsarten kann beispielsweise durch entsprechende Codierungen von Schlüsseln befugten Personen Zugang zum Gefahrenbereich gewährt werden, beispielsweise um dort Reparatur- oder Installationsarbeiten durchzuführen. Je nach Betriebsart kann dann die Maschine 3 komplett angehalten oder in einem eingeschränkten Betriebsmodus, beispielsweise mit reduzierter Geschwindigkeit, gefahren werden.

[0042] Erfindungsgemäß kann über die Eingabeeinheit 10 eine fehlersichere Auswahl einer Betriebsart vorgenommen werden. Die hierfür erforderlichen Verfahrensschritte sind im Ablaufdiagramm der Figuren 2a - f zusammengefasst.

[0043] In einem ersten Schritt (Schritt Nr. 1 in Figur 2a) wird ein Schlüssel in den Schlüsseleinsatz des elektronischen Schlüsselsystems 6 gesteckt, so dass der Schlüsseleinsatz berührungslos die Daten des Schlüssels ausliest.

[0044] Durch das Einstecken des Schlüssels wird dann, wenn dieser vom Schlüsseleinsatz als gültiger Schlüssel erkannt wird, der Schaltzustand des Schaltsignals am Schaltausgang LA auf den Wert 1 gesetzt (Schritt Nr. 2). Dieses die Anwesenheit eines gültigen Schlüssels signalisierende Schaltsignal wird über den Schalteingang SI in die Sicherheitssteuerung 4 eingelesen.

[0045] Die vom Schlüsseleinsatz gelesenen Daten des Schlüssels werden hinsichtlich ihres Formats geprüft und dann, wenn diese Prüfung erfolgreich war, über den Datenausgang 7 eingelesen (Schritt Nr. 3).

[0046] Mit dem Setzen des Schaltsignals auf den Wert 1, welches in die Sicherheitssteuerung 4 eingelesen wird, wird in der Sicherheitssteuerung 4 kontrolliert, ob die am Datenausgang 7 ausgelesenen Daten innerhalb eines vorgegebenen Zeitintervalls in die nichtfehlersichere Steuerung 5 eingelesen werden. Hierzu wird in der Sicherheitssteuerung 4 eine Zeiterwartung gestartet (Schritt Nr. 4). Dabei wird ein Zeitintervall vorgegebener Länge geöffnet und abgeprüft, ob innerhalb dieses Zeitintervalls die Daten des Schlüssels in die nichtfehlersichere Steuerung 5 eingelesen werden.

[0047] Dieses Einlesen (Schritt Nr. 5) erfolgt über die Busleitungen 8a des Bussystems. Dabei werden in bekannter Weise die Daten in einem festgelegten Eingangsbereich der nichtfehlersicheren Steuerung 5 eingelesen und dann in einen festgelegten Datenbereich der nichtfehlersicheren Steuerung 5 umkopiert.

[0048] Als erste Fehlerkontrolle erfolgt in der nichtfehlersicheren Steuerung 5 eine Berechnung der Prüfsumme der Daten des Schlüssels (Schritt Nr. 6). Darauf wird geprüft, ob die Prüfsumme in Ordnung ist, das heißt ob sie einem zulässigen Wert entspricht (Schritt Nr. 7).

[0049] Als weitere Fehlerkontrolle wird in der Sicherheitssteuerung 4 geprüft, ob die Daten des elektronischen Schlüsselsystems 6 innerhalb des die Zeiterwartung definierenden Zeitintervalls in die nichtfehlersichere Steuerung 5 eingelesen werden. Da diese Daten nur in die nichtfehlersichere Steuerung 5 eingelesen werden, wird nach in der nichtfehlersicheren Steuerung 5 erfolgter Prüfsummenberechnung eine Berechtigungsstufe in der Variablen mit dem symbolischen Namen Read-Authorization für die eingelesenen Daten vergeben und in ein Merkerwort MW01 oder einen dementsprechenden Datenbereich eingeschrieben, das von der nichtfehlersicheren Steuerung 5 an die Sicherheitssteuerung 4 gesendet wird. Ein derartiges Merkerwort bildet ein von der Sicherheitssteuerung 4 lesbares Datenformat. Anhand dieses Merkerworts MW01 erfolgt dann in der Sicherheitssteuerung 4 die Prüfung, ob die Daten des Schlüssels innerhalb der Zeiterwartung empfangen wurden (Schritte Nr. 8 - 10).

[0050] Wird bei der Prüfsummenberechnung oder der Überwachung der Zeiterwartung ein Fehler festgestellt, so erfolgt eine Verzweigung in eine Fehlerverrastung. Bei Verzweigen in eine Fehlerverrastung wird die Betriebsartwahl sofort gestoppt und kann nur dann fortgesetzt werden, wenn der Benutzer eine vorgegebene Aktion durchführt, beispielsweise eine spezifische Eingabe am Touchscreen vornimmt.

[0051] Mit den vorgenannten Fehlerkontrollen kann kontrolliert werden, ob das elektronische Schlüsselsys-

tem 6 und das Steuerungssystem 2, insbesondere die nichtfehlersichere Steuerung 5, korrekt arbeiten. Insbesondere kann auf diese Weise geprüft werden, ob im Schlüsseleinsatz überhaupt ein Schlüssel vorhanden ist. Ist nämlich kein Schlüssel im Schlüsseleinsatz vorhanden, werden keine Daten in die Sicherheitssteuerung 4 übertragen, so dass dann die Prüfsumme den unzulässigen Wert Null annimmt, wodurch eine Verzweigung in die Fehlerverrastung erfolgt.

[0052] Entspricht die Prüfsumme einem zulässigen Wert, so wird die Berechtigungsstufe von der Sicherheitssteuerung 4 an die Eingabeeinheit 10 gesendet (Schritt Nr. 11), wodurch die Eingabeeinheit 10 für die Auswahl einer Betriebsart freigegeben wird (Schritt Nr. 12). In der Eingabeeinheit 10 wird hierzu vorteilhaft ein Bild aufgebaut, über welches ein Benutzer eine Betriebsart auswählen kann.

[0053] Die vom Benutzer ausgewählte Betriebsart wird in der Eingabeeinheit 10 der Variablen mit dem symbolischen Namen Select-MSO zugewiesen und dann an die nichtfehlersichere Steuerung 5 gesendet. In der nichtfehlersicheren Steuerung 5 wird die gewählte Betriebsart in das Merkerwort MW03 kopiert, das von der Sicherheitssteuerung 4 gelesen werden kann. Dieses Merkerwort MW03 wird dann von der nichtfehlersicheren Steuerung 5 an die Sicherheitssteuerung 4 gesendet (Schritt Nr. 14).

[0054] In der Sicherheitssteuerung 4 wird weiterhin abgefragt, ob von der nichtfehlersicheren Steuerung 5 neue Daten übersendet werden. Dies wird in der Sicherheitssteuerung 4 dadurch festgestellt, dass im Merkerwort MW01 ein Wert ungleich Null erscheint (Schritt Nr. 15).

[0055] Schließlich wird in den Schritten Nr. 16 und 17 in der Sicherheitssteuerung 4 geprüft, ob im Merkerwort MW03 ein zulässiger Code erscheint, und damit, ob die gewählte Betriebsart in einem zulässigen Bereich liegt (Schritte Nr. 16, 17).

[0056] Hierzu ist in der Sicherheitssteuerung 4 eine Liste zulässiger Betriebsarten hinterlegt. Dann kann in der Sicherheitssteuerung 4 durch einen einfachen Vergleich des eingelesenen Merkerworts MW03 mit der gespeicherten Liste ermittelt werden, ob eine zulässige Betriebsart gewählt worden ist.

[0057] Liegt keine zulässige Betriebsart vor, erfolgt eine Verzweigung in eine Fehlerverrastung.

[0058] Liegt jedoch eine zulässige Betriebsart vor, so wird in der Sicherheitssteuerung 4 die zulässige Betriebsart, das heißt der Inhalt des Merkerworts MW03 in das Merkerwort MW05 kopiert, das dann an die nichtfehlersichere Steuerung 5 gesendet wird (Schritte Nr. 18, 19).

[0059] Dieses Merkerwort MW05 wird dann von der nichtfehlersicheren Steuerung 5 an die Eingabeeinheit 10 gesendet. Dort wird die ausgewählte Betriebsart dem Benutzer angezeigt (Schritt Nr. 20). Diese Anzeige erfolgt in einem anderen Bild als in dem Bild, in dem der Benutzer die Betriebsartauswahl vorgenommen hat. Dies ist eine Voraussetzung für ein sicheres Rücklesen der ausgewählten Betriebsart. Eine zweite Voraussetzung hierfür ist, dass das Rücklesen, in eine Variable (hier MW05) erfolgt, die von der Variable für das Einlesen der Betriebsart (hier MW03) verschieden ist.

[0060] Sobald dem Benutzer die ausgewählte Betriebsart durch das Rücklesen auf die Eingabeeinheit 10 angezeigt wurde, muss die Auswahl vom Benutzer durch eine Eingabe an der Eingabeeinheit 10 bestätigt werden (Schritt Nr. 21).

[0061] Bei einer negativen Bestätigung wird in der Eingabeeinheit 10 eine Fehlervariable mit dem symbolischen Namen ErrorMS0 gesetzt, wodurch eine Verzweigung in eine Fehlerverrastung erfolgt (Schritt Nr. 23).

[0062] Bei einer positiven Bestätigung wird in der Eingabeeinheit 10 eine Variable mit dem symbolischen Namen SwitchMS0 gesetzt (Schritt Nr. 22) und über das Bussystem an die nichtfehlersichere Steuerung 5 gesendet. Die so gewählte Betriebsart wird dann in das Merkerwort MW07 kopiert und an die Sicherheitssteuerung 4 gesendet (Schritt Nr. 24).

[0063] In der Sicherheitssteuerung 4 erfolgt dann ein Vergleich, ob die ausgewählte Betriebsart (enthalten im Merkerwort MW03) der bestätigten Betriebsart (enthalten im Merkerwort MW07) entspricht (Schritt Nr. 25).

[0064] Sind diese Werte unterschiedlich, erfolgt eine Verzweigung in eine Fehlerverrastung.

[0065] Sind jedoch beide Werte identisch, führt die Sicherheitssteuerung 4 eine Umschaltung auf die ausgewählte Betriebsart durch, wobei hierzu von der Sicherheitssteuerung 4 entsprechende Ausgänge des Steuerungssystems 2 gesetzt werden (Schritt Nr. 26).

[0066] Die gesamte beschriebene Kette wird ebenfalls durchlaufen, wenn der Schlüssel herausgezogen wird. Hierbei müssen alle Variablen den Wert 0 annehmen. Der Ausgang LA muss zeitglich zurückgesetzt werden. Somit wird durch Prüfung in der sicheren Steuerung 4 sichergestellt, dass keine Werte in den nicht sicheren Teilen der Steuerung 5 sowie des Eingabesystems 10 gespeichert bleiben können. Damit erfolgt eine Funktionskontrolle aller Komponenten des Sicherheitssystems 1.

Bezugszeichenliste

[0067]

(1)	Sicherheitssystem
(2)	Steuerungssystem
(3)	Maschine
(4)	Sicherheitssteuerung
(5)	nichtfehlersichere Steuerung
(6)	elektronisches Schlüsselsystem
(7)	Datenausgang
(8a-b)	Busleitung
(9a-c)	Leitung
(10)	Eingabeeinheit
(LA)	Schaltausgang
(SI)	Schalteingang

Patentansprüche

1. Verfahren zur Einstellung einer Betriebsart eines Sicherheitssystems (1), umfassend ein Zugangssystem, welches an ein eine Maschine steuerndes Steuerungssystem (2) angeschlossen ist, wobei das Steuerungssystem (2) eine Sicherheitssteuerung (4) aufweist, **gekennzeichnet durch** folgende Verfahrensschritte:

   • Zweikanaliges Auslesen von Signalen des Zugangssystems in das Steuerungssystem (2)
   • Durchführen einer Gültigkeitsüberprüfung der Signale des Zugangssystems in dem Steuerungssystem (2)
   • wobei das Steuerungssystem (2) nur bei Vorliegen gültiger Signale des Zugangssystems die Auswahl einer Betriebsart über die Eingabeeinheit (10) freigibt.
   • Durchführen einer Fehlerkontrolle der Auswahl der Betriebsart in der Sicherheitssteuerung (4)
   • Umschalten auf die ausgewählte Betriebsart **durch** die Sicherheitssteuerung (4) nach positiv durchgeführter Fehlerkontrolle.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** das Zugangssystem eine diversitäre Ausgangsstruktur aufweist.

3. Verfahren nach einem der Ansprüche 1 oder 2, **dadurch gekennzeichnet, dass** die Signale wenigstens eines Ausgangs des Zugangssystems in der Sicherheitssteuerung (4) für eine Gültigkeitsüberprüfung herangezogen werden.

4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, dass** das Sicherheitssystem (1) zusätzlich zu der Sicherheitssteuerung (4) eine nichtfehlersichere Steuerung (5) aufweist, wobei die nichtfehlersichere Steuerung (5) die Eingabeeinheit (10) steuert, und wobei die Signale eines ersten Ausgangs des Zugangssystems in die nichtfehlersichere Steuerung (5) und die Signale des zweiten Ausgangs des Zugangssystems in die Sicherheitssteuerung (4) eingelesen werden.

5. Verfahren nach Anspruch 4, **dadurch gekennzeichnet, dass** das Zugangssystem von einem elektronischen Schlüsselsystem (6), umfassend einen Schlüsseleinsatz und wenigstens einen Schlüssel, gebildet ist, dass das Zugangssystem einen Datenausgang (7) aufweist, über welchen Daten eines im Schlüsseleinsatz befindlichen Schlüssels in die nichtfehlersichere Steuerung (5) eingelesen werden, und dass das Zugangssystem einen Schaltausgang (LA) aufweist, über welchen ein Schaltsignal, dessen Schaltzustände angeben, ob ein Schlüssel im Schlüsseleinsatz vorhanden ist oder nicht, in die Sicherheitssteuerung (4) eingelesen wird.

6. Verfahren nach Anspruch 5, **dadurch gekennzeichnet, dass** als erste Gültigkeitsüberprüfung von Signalen des Zugangssystems bei Einlesen eines Schaltsignals, dessen Schaltzustand einen im Schlüsseleinsatz befindlichen Schlüssel signalisiert, in der Sicherheitssteuerung (4) eine Zeiterwartung durch Öffnen eines Zeitintervalls gestartet wird, und dass in der Sicherheitssteuerung (4) geprüft wird, ob innerhalb dieses Zeitintervalls Daten des Schlüssels über den Datenausgang (7) in die nichtfehlersichere Steuerung (5) eingelesen wurden.

7. Verfahren nach Anspruch 6, **dadurch gekennzeichnet, dass** als zweite Gültigkeitsüberprüfung eine Prüfsummenberechnung der vom Datenausgang (7) eingelesenen Daten des Schlüssels in der nichtfehlersicheren Steuerung (5) durchgeführt wird.

8. Verfahren nach Anspruch 7, **dadurch gekennzeichnet, dass** die nichtfehlersichere Steuerung (5) nach erfolgreicher Gültigkeitsüberprüfung ein Autorisierungssignal an die Eingabeeinheit (10) sendet, wodurch Eingaben an der Eingabeeinheit (10) freigegeben werden.

9. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, dass** die Eingabeeinheit (10) von einem Touchscreen gebildet ist.

10. Verfahren nach Anspruch 9, **dadurch gekennzeichnet, dass** nach Empfang des Autorisierungssignals im Touchscreen ein Bild aufgebaut oder zugänglich gemacht wird, in welchem eine Betriebsart ausgewählt werden kann.

11. Verfahren nach einem der Ansprüche 1 bis 10, **dadurch gekennzeichnet, dass** in der nichtfehlersicheren Steuerung (5) als Fehlerkontrolle geprüft wird, ob die ausgewählte Betriebsart in einem zulässigen Bereich liegt.

12. Verfahren nach einem der Ansprüche 1 bis 11, **dadurch gekennzeichnet, dass** zur Fehlerkontrolle einer ausgewählten Betriebsart diese auf die Eingabeeinheit (10) rückgelesen wird.

13. Verfahren nach Anspruch 12, **dadurch gekennzeichnet, dass** die ausgewählte Betriebsart und die rückgelesene Betriebsart in unterschiedlichen Bildern der Eingabeeinheit (10) angezeigt werden.

14. Verfahren nach einem der Ansprüche 1 bis 13, **dadurch gekennzeichnet, dass** bei Aufdeckung eines Fehlers in dem Steuerungssystem (2) eine Fehlerverrastung erzeugt wird.

15. Verfahren nach einem der Ansprüche 5 bis 14, **dadurch gekennzeichnet, dass** bei Zielen eines Schlüssels aus dem Schlüsseleinsatz des Schlüsselsystems (6) eine Funktionskontrolle aller Komponenten des Sicherheitssystems (1) durchgeführt wird.

16. Sicherheitssystem umfassend ein Zugangssystem, welches an ein eine Maschine steuerndes Steuerungssystem (2) angeschlossen ist, wobei das Steuerungssystem (2) eine nichtfehlersichere Steuerung (5) aufweist, **dadurch gekennzeichnet, dass** das Zugangssystem eine zweikanalige Ausgangsstruktur aufweist, welches ausgebildet ist, Signale in das Steuerungssystem (2) auszulesen, dass das Steuerungssystem (2) ausgebildet ist, eine Gültigkeitsüberprüfung der Signale des Zugangssystems durchzuführen, wobei das Steuerungssystem (2) ausgebildet ist, die Auswahl einer Betriebsart über die Eingabeeinheit (10) freizugeben, falls gültige Signale des Zugangssystems vorliegen, dass die Sicherheitssteuerung (4) ausgebildet ist, eine Fehlerkontrolle der Auswahl der Betriebsart durchzuführen, und dass die Sicherheitssteuerung (4) ausgebildet ist, nach positiv durchgeführter Fehlerkontrolle eine Umschaltung auf die ausgewählte Betriebsart vorzunehmen.

Fig. 1

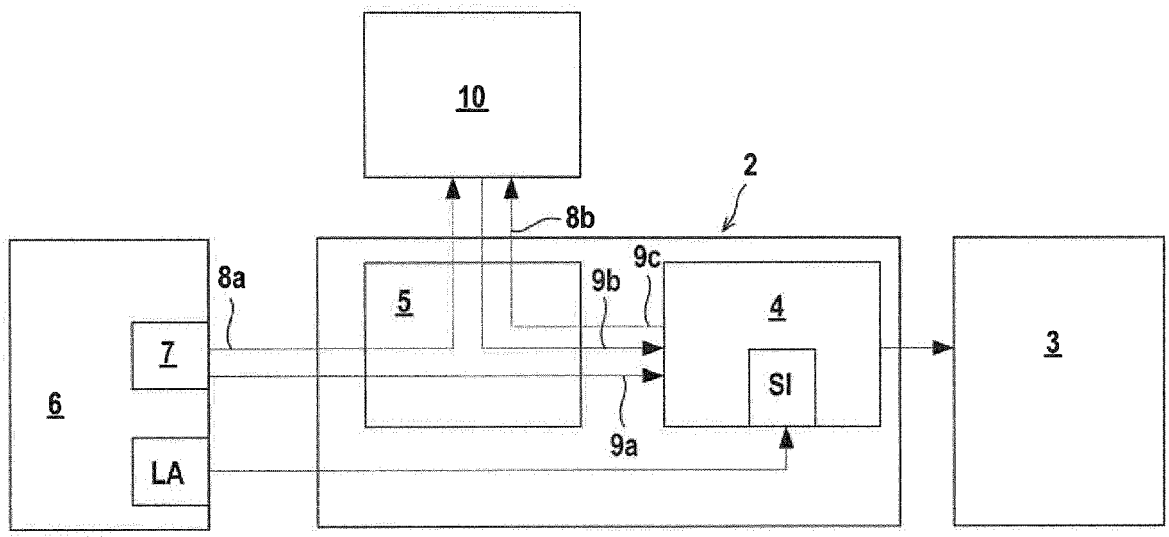


Fig. 2a

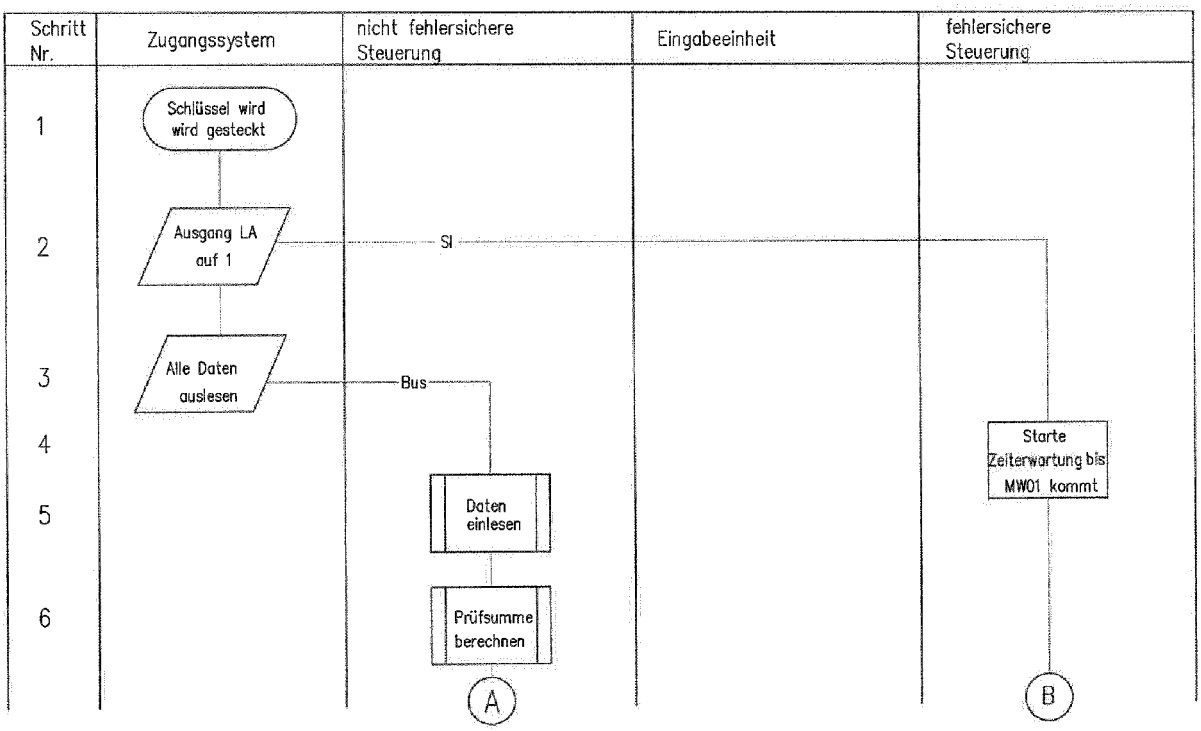

Schritt Nr.
Zugangssystem
nicht fehlersichere Steuerung
Eingabeeinheit
fehlersichere Steuerung
1
2
3
4
5
6
Schlüssel wird wird gesteckt
Ausgang LA auf 1
SI
Alle Daten auslesen
Bus
Daten einlesen
Prüfsumme berechnen
A
Starte Zeiterwartung bis MW01 kommt
B

Fig. 2b

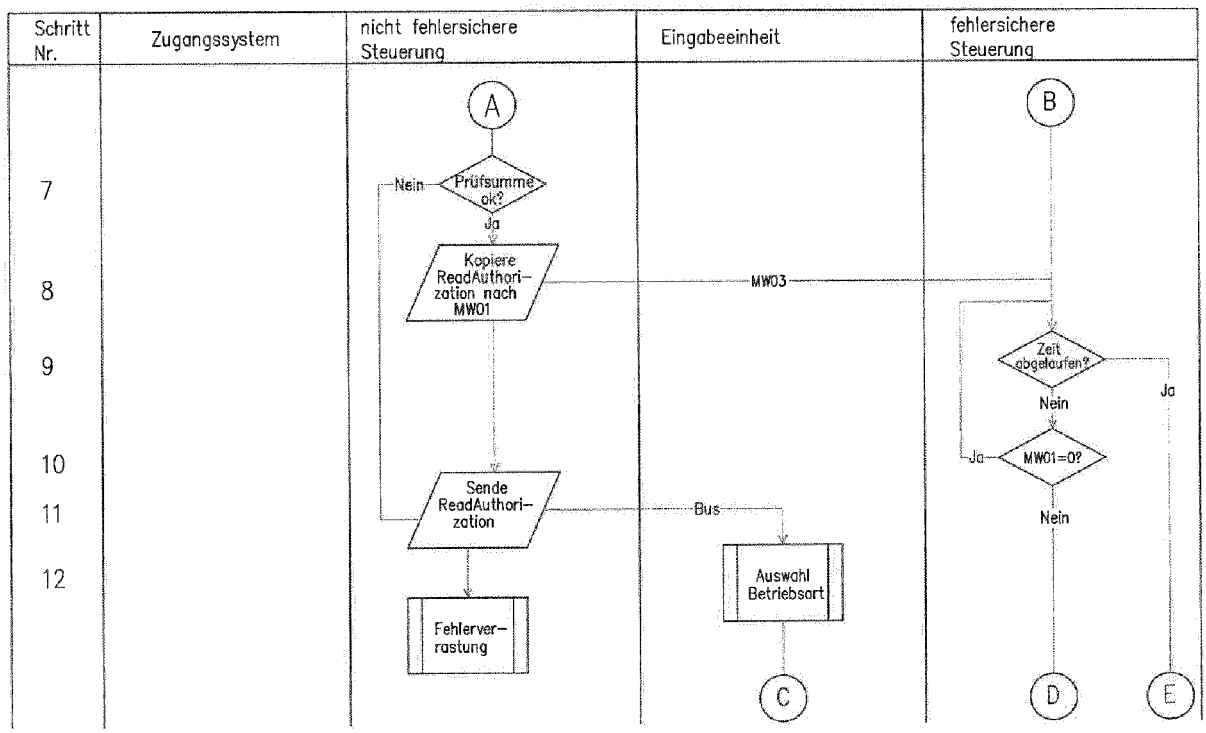

Schritt Nr.
Zugangssystem
nicht fehlersichere Steuerung
Eingabeeinheit
fehlersichere Steuerung
A
B
7
Nein
Prüfsumme ok?
Ja
8
Kopiere ReadAuthori-zation nach MW01
MW03
9
Zeit abgelaufen?
Nein
Ja
10
Ja
MW01=0?
11
Sende ReadAuthori-zation
Bus
Nein
12
Auswahl Betriebsart
Fehlerver-rastung
C
D
E

Fig. 2c

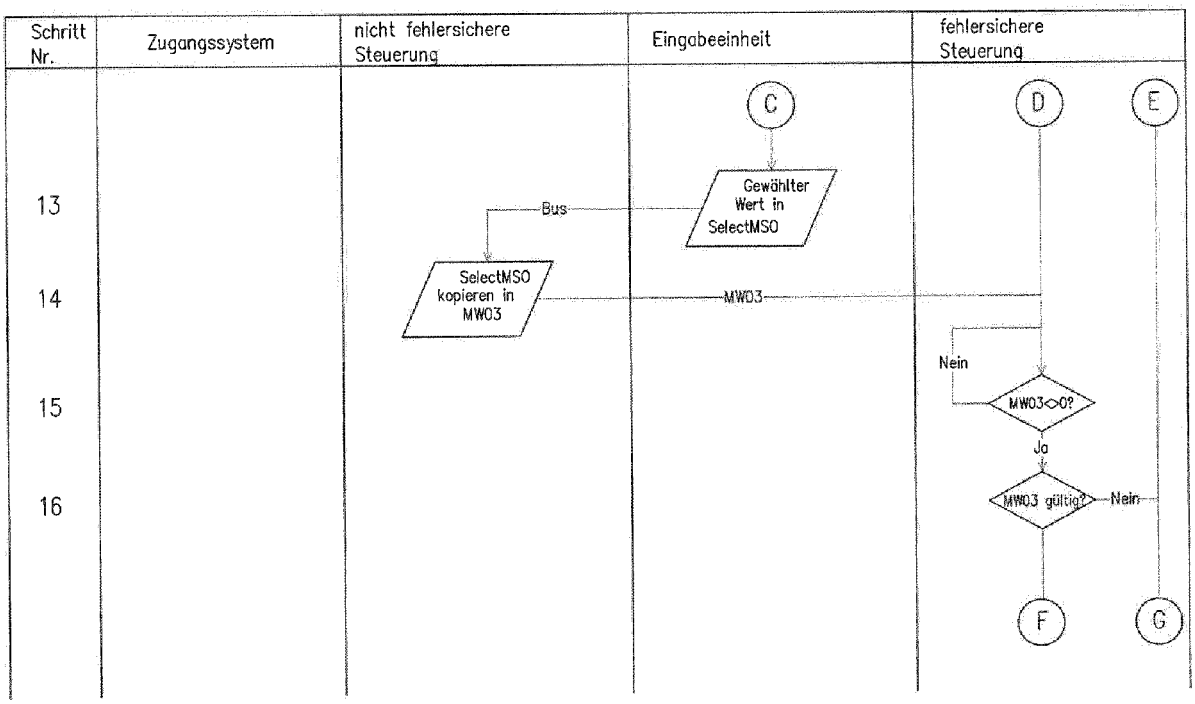

Schritt Nr.
Zugangssystem
nicht fehlersichere Steuerung
Eingabeeinheit
fehlersichere Steuerung
C
D
E
13
Gewählter Wert in SelectMSO
Bus
14
SelectMSO kopieren in MW03
MW03
Nein
15
MW03<>0?
Ja
16
MW03 gültig?
Nein
F
G

Fig. 2d

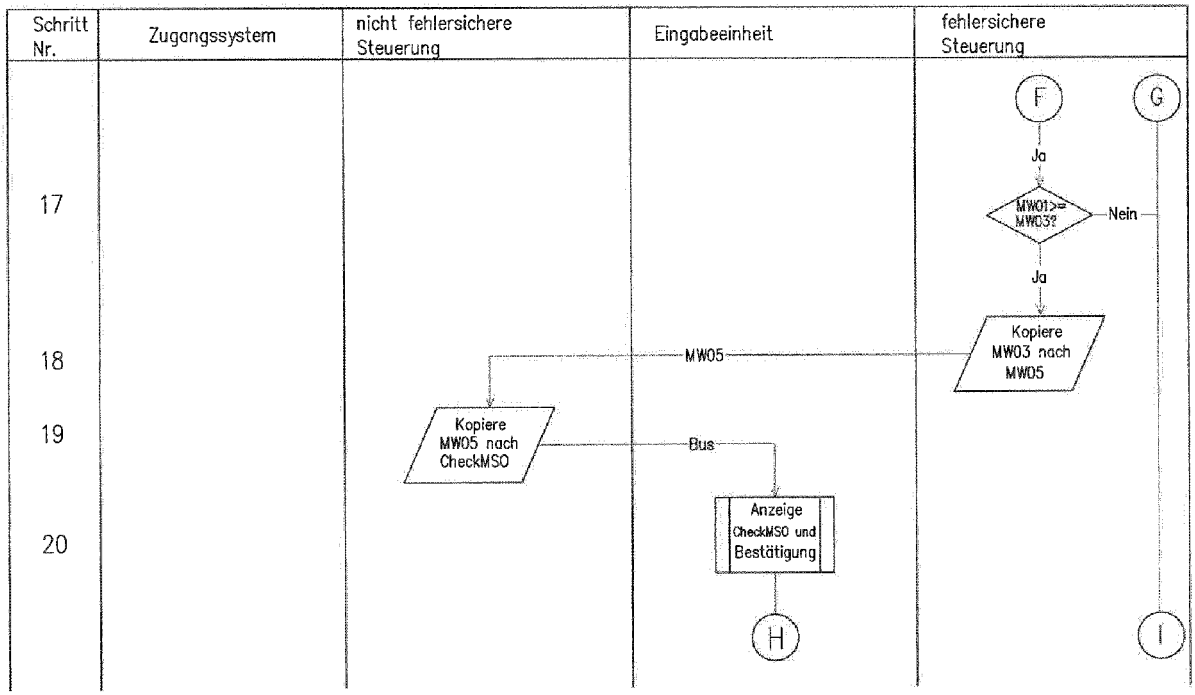

Schritt Nr.
Zugangssystem
nicht fehlersichere Steuerung
Eingabeeinheit
fehlersichere Steuerung
17
18
19
20
F
G
Ja
MW01>= MW03?
Nein
Ja
Kopiere MW03 nach MW05
MW05
Kopiere MW05 nach CheckMS0
Bus
Anzeige CheckMS0 und Bestätigung
H
I

Fig. 2e

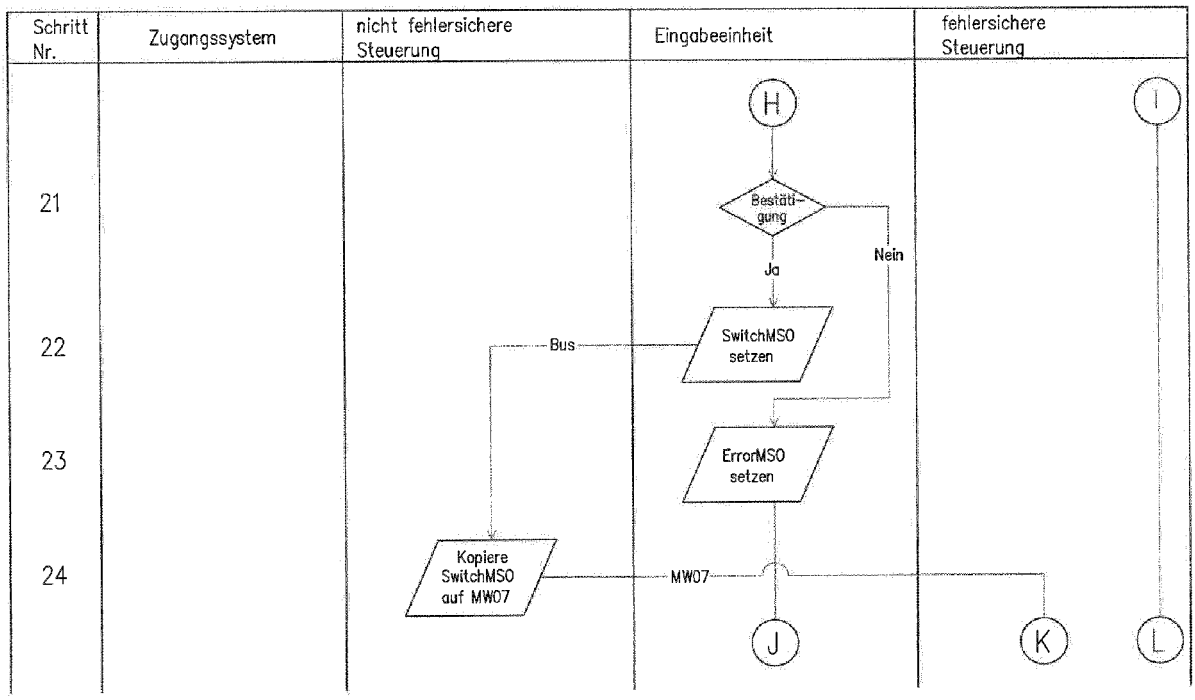
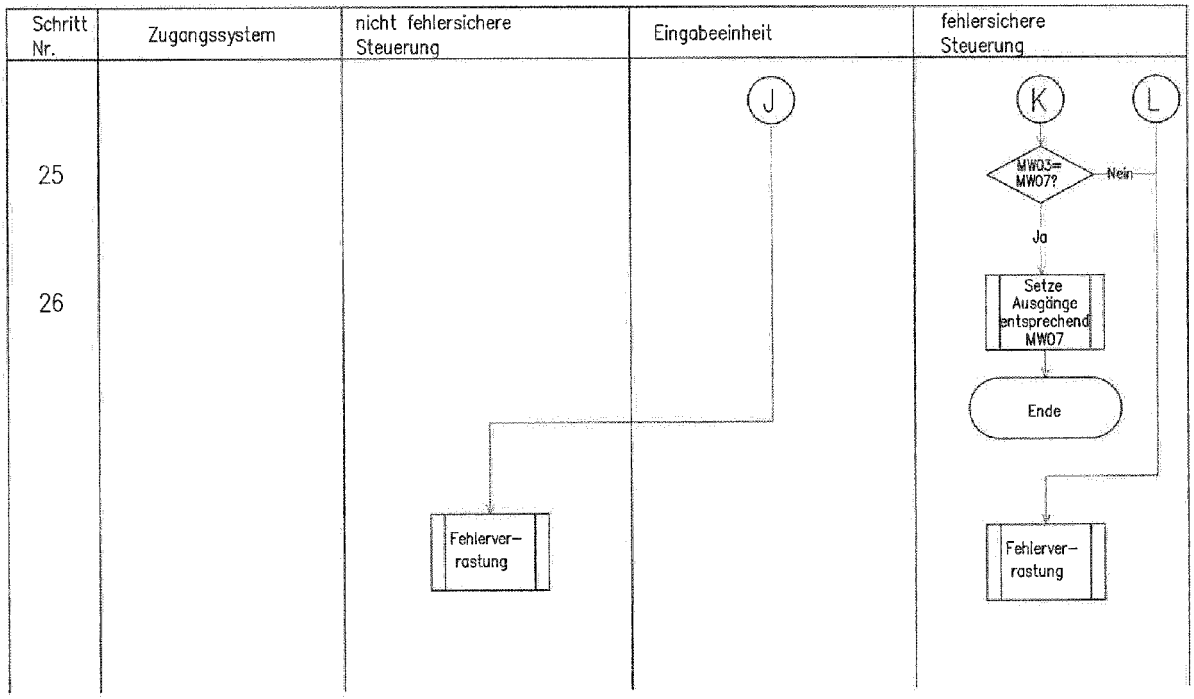

Schritt Nr.
Zugangssystem
nicht fehlersichere Steuerung
Eingabeeinheit
fehlersichere Steuerung
21
22
23
24
H
I
Bestäti-gung
Nein
Ja
SwitchMSO setzen
Bus
ErrorMSO setzen
Kopiere SwitchMSO auf MW07
MW07
J
K
L

Fig. 2f


Schritt Nr.
Zugangssystem
nicht fehlersichere Steuerung
Eingabeeinheit
fehlersichere Steuerung
25
26
J
K
L
MW03= MW07?
Nein
Ja
Setze Ausgänge entsprechend MW07
Ende
Fehlerver-rastung
Fehlerver-rastung