



(12)

EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
08.09.2004 Patentblatt 2004/37

(51) Int Cl.7: **B41F 33/00**

(21) Anmeldenummer: **04102212.0**

(22) Anmeldetag: **26.02.1999**

(84) Benannte Vertragsstaaten:
BE CH DE FR GB IT LI NL

(30) Priorität: **25.02.1999 DE 19908230**

(62) Dokumentnummer(n) der früheren Anmeldung(en)
nach Art. 76 EPÜ:
99103804.3 / 1 031 420

(71) Anmelder: **Heidelberger Druckmaschinen
Aktiengesellschaft
69115 Heidelberg (DE)**

(72) Erfinder:
• **Janzer, Reinhard IP Heildelberger
76646, Bruchsal (DE)**

- **Albrecht, Kai
69124, Heidelberg (DE)**
- **Grimm, Ulrich
IP Heidelberger Druckmaschinen AG
69234, Dielheim (DE)**
- **Pritschow, Michael
69168, Wiesloch (DE)**
- **Roessler, Georg
74918, Angelbachtal (DE)**
- **Wagner, Andreas
76676, Graben-Neudorf (DE)**

Bemerkungen:

Diese Anmeldung ist am 19 - 05 - 2004 als
Teilanmeldung zu der unter INID-Kode 62
erwähnten Anmeldung eingereicht worden.

(54) **Vorrichtung zur Überwachung von sicherheitsrelevanten Vorgängen an Maschinen**

(57) Die Erfindung betrifft eine Vorrichtung und ein Verfahren zur Überwachung sicherheitsrelevanter Vorgänge an Stell-/Antriebsselementen von Maschinen. Der sicherheitsrelevante Vorgang wird durch mindestens eine Sicherheits Ein-/Ausgabeeinrichtung (4) und eine zentrale Sicherheitsüberwachungssteuerung (6) überwacht. Die Sicherheits Ein-/Ausgabeeinrichtung (4), die Sicherheitsüberwachungssteuerung (6) und die Betriebssteuerung (1) der Maschine sind mittels Feldbus-system (2) miteinander verbunden.

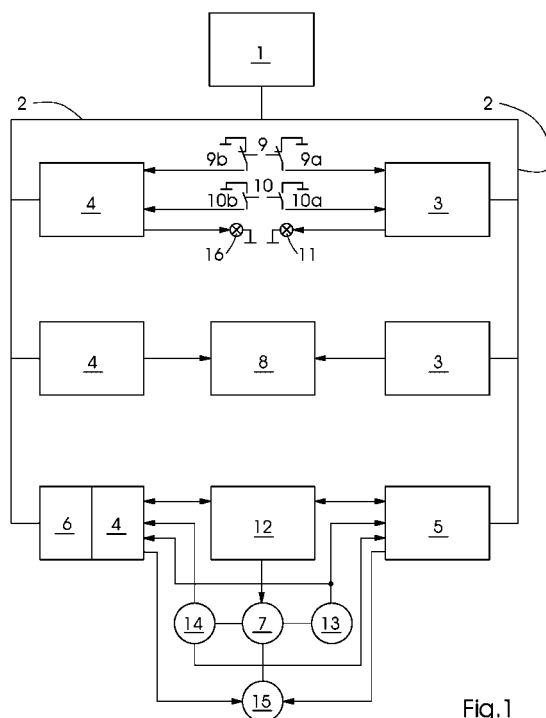


Fig.1

Beschreibung

[0001] Im Bereich des Maschinenbaus, insbesondere im Druckmaschinenbau ist es seitens der Berufsgenossenschaften erforderlich, daß sicherheitsrelevante Vorgänge an den Maschinen einfehlersicher laufen müssen. Das heißt, eine Steuerung oder ein Teil von ihr ist einfehlersicher, wenn ein einzelner Fehler in der Steuerung zu keiner Gefahr führt. Schaltungstechnisch bedeutet dies, daß bestimmte Funktionen doppelt, das heißt redundant vorhanden sein müssen.

[0002] Bei der Steuerung der Fa. Heidelberger Druckmaschinen AG (CP-Tronic) erfolgt dieses dadurch, daß in der Steuerung ein zentrales Sicherheitsmodul vorgesehen ist, in welches Zustände von sicherheitsrelevanten Vorgängen parallel zu den Steuerungsmodulen eingelesen werden. Dabei wird zur Betätigung eines sicherheitsrelevanten Vorgangs ein Schalter mit jeweils einem Öffner und einem Schließer in zwei getrennte Systemen eingelesen bzw. überwacht. Das heißt eine Leitung führt zu dem Steuerungsmodul und eine zweite redundante Leitung führt zu einem zentralen Sicherheitsmodul. Der sicherheitsrelevante Vorgang wird nur ausgelöst, wenn sowohl im Steuerungsmodul, als auch im Sicherheitsmodul eine gleichzeitige Auslösung beider Kontakte erkannt wird.

[0003] Der Hauptantrieb der Maschine wird ebenso von zwei redundant aufgebauten Systemen überwacht und im Falle einer Nichtübereinstimmung sicherheitsrelevanter Zustände erfolgt eine Abschaltung des Antriebs. Zum redundanten Aufbau gehören zwei Rechner, von denen einer die Steuerung des Hauptantriebs übernimmt und der andere die eigentliche Maschinensteuerung. Bei Ausfall des eigentlichen Hauptantriebsrechners übernimmt der Rechner für die Maschinensteuerung die Steuerungsfunktion des Antriebsrechners und führt den Hauptantrieb kontrolliert zum Stillstand. Zusätzlich werden über ein Sicherheitsmodul verschiedene Schutzkontakte, Notastaster ect. eingelesen, die einerseits über eine Eingabekarte mittelbar dem Antriebsrechner und redundant dazu über direkte Pin-Eingänge am Antriebsrechner ebenso dem Antriebsrechner zugeleitet. Weiterhin werden die Ist-Werte des HauptAntriebsselements über zwei getrennte Inkrementalgeber eingelesen, von denen der eine am Motor direkt und der andere an einem drehenden Teil der Druckmaschine, beispielsweise am Plattenzylinder angebracht ist. Die Signale des ersten Inkrementalgebers am Motor werden über separate Signalleitungen dem Antriebsrechner zugeführt und die Signale des Inkrementalgebers am Plattenzylinder ebenfalls über separate Signalleitungen sowohl dem Antriebsrechner, als auch dem Rechner für die Maschinensteuerung.

[0004] Nachteilig an dieser Technologie ist, daß von allen sicherheitsrelevanten Einrichtungen jeweils eine Leitung an die eigentlichen Steuermodule und eine zusätzliche Leitung zum zentralen Sicherheitsmodul geführt werden muß, um das Einlesen des Zustandes red-

undant zu halten. Diese Lösung ist einerseits aufwendig und teuer und bietet andererseits nur beschränkte Erweiterungsmöglichkeiten. Die Erweiterungsmöglichkeiten sind mit ebenfalls hohem Aufwand an Leitungen verbunden und eine Erweiterung ist nur soweit möglich, wie das zentrale Sicherheitsmodul freie Eingänge zum Einlesen des sicherheitsrelevanten Zustandes bietet.

[0005] Aus dem Stand der Technik ist weiterhin die DE 195 29 430 A1 bekannt, die zur Überwachung von elektrischen Antriebssystemen insbesondere an Druckmaschinen mit Mehrfachantrieben sogenannte Sicherheitsmodule vorschlägt. Diese Sicherheitsmodule bestehen daraus, daß sie vorwiegend als Software realisiert sind und insgesamt drei Komponenten aufweisen. Diese drei Komponenten sind, die Fehlererkennung und -diagnose, die Entscheidungsfindung aufgrund Fehlerart und -größe und die Reaktions- bzw. Maßnahmenleitung. Diese Sicherheitsmodule haben einen Zugriff auf Signale im Bereich der Funktionsteile, wie z.B. drehende Zylinder der Druckmaschine, im Bereich der Elektromotoren, der Leistungselektronik, der Signalverarbeitungseinheit und der Netzteile und sind zu deren Vergleich oder Auswertung auf Plausibilität ausgebildet.

[0006] Nachteilig an dem Stand der Technik gemäß der DE 195 29 430 A1 ist, daß neben den Überwachungen der Antriebe keine weiteren Überwachungen für sonstige sicherheitsrelevante Vorgänge berücksichtigt werden. Das heißt, es können keine sicherheitsrelevanten Eingänge eingelesen und keine redundanten Sicherheitsausgänge gesetzt werden.

[0007] Ausgehend von diesem Stand der Technik ist die Aufgabe der Erfindung darin zu sehen, eine kostengünstigere Lösung zu schaffen, mit der eine Erweiterung von sicherheitsrelevanten Funktionen möglich ist, ohne zusätzlichen Kabelaufwand. Weiterhin besteht die Aufgabe der Erfindung darin, daß bei der Vereinfachung gleichzeitig die durch die BG vorgeschriebenen Bedingungen eingehalten werden.

[0008] Die Aufgabe wird erfindungsgemäß durch die Merkmale der Vorrichtung bzw. Verfahrensansprüche 1 bzw. 8 gelöst. Vorteilhafte Ausgestaltungen ergeben sich durch die abhängigen Ansprüche 2-7 und 9-11

[0009] Der Vorteil der Erfindung besteht darin, daß das Einlesen der für die Sicherheit relevanten Zustände nicht zentral an einer mittels Leitung erreichbaren Stelle stattfindet, sondern dezentral unmittelbar an der Stelle, an der der Zustand erzeugt, bzw. verändert wird. Das heißt, ein für die Übermittlung dieser Zustandssignale installiertes Bussystem, wird entlang der Druckmaschine verlegt und verbindet mehrere vor Ort angebrachte Sicherheits Ein-/Ausgabeeinrichtungen mit einer oder mehreren, für einen sicherheitskritischen Bereich verantwortlichen Sicherheitsüberwachungssteuerungen. Die Verbindung zu dem Bussystem erfolgt auf kürzestem Wege von dem Ort, an den der sicherheitsrelevante Zustand eingelesen wird. Eine einfache Erweiterung auf die zusätzlichen Überwachung weiterer sicherheitsrelevanter Zustände ist dadurch möglich, daß jeweils als

modulbauweise konzipierte Sicherheitsüberwachungssteuerungen und Sicherheitseinleseinrichtung überall an das Bussystem angeschlossen werden können.

[0010] Die Sicherheits Ein-/Ausgabeeinrichtungen sind beispielsweise vor Ort da angebracht, wo sich Notastaster oder sogenannte Endschalter einer Schutzeinrichtung befinden. Weiterhin fragt die Sicherheitseinlesevorrichtung auch analoge Signale ab wie beispielsweise die Temperatur eines Trockners, welche bei Überschreiten eines Maximalwertes eine Abschaltung bewirken kann. Die Sicherheits Ein-/Ausgabeeinrichtung liest die Zustandsände der Notastaster, Endschalter oder Temperaturfühler ein und übermittelt diese mittels Bussystem an eine Sicherheitsüberwachungssteuerung. Die Sicherheitsüberwachungssteuerung ist beispielsweise an einem Antriebselement vor Ort angebracht der eine kontinuierliche oder diskontinuierliche sicherheitskritische Bewegung ausführt. Die Bewegung ist deshalb sicherheitskritisch, weil eine Bedienperson in dessen Gefahrenbereich gelangen kann. Zwischen Antriebselement und Sicherheitsüberwachungssteuerung ist ebenfalls eine Sicherheits Ein-/Ausgabeeinrichtung geschaltet, welche die sicherheitsrelevanten Signale des Antriebselements einliest und diese der Sicherheitsüberwachungssteuerung mitteilt. Die Sicherheits Ein-/Ausgabeeinrichtung und die Sicherheitsüberwachungssteuerung kann in diesem Fall in eine Einheit integriert sein.

[0011] Die Sicherheits Ein-/Ausgabeeinrichtung legt ihren eingelesenen Zustand auf das Bussystem wodurch alle am Bussystem befindlichen Sicherheitsüberwachungssteuerungen auf die gemeldete Nachricht Zugriff haben. Diesen Vorgang bezeichnet man als broadcast. Ob eine Sicherheitsüberwachungssteuerung an der gemeldeten Nachricht interessiert ist, entscheidet diese für sich selbst. Das heißt, die Nachricht wird ignoriert, wenn der gemeldete sicherheitskritische Zustand für den von der Sicherheitsüberwachungssteuerung überwachten Antrieb nicht relevant ist. Es werden aber entsprechende Maßnahmen durchgeführt, wenn der gemeldete sicherheitskritische für den von der Sicherheitsüberwachungssteuerung überwachten Antrieb relevant ist. Somit übernimmt jede Sicherheitsüberwachungssteuerung abhängig von deren Verantwortung nur das wesentliche. Durch das gezielte Auswerten, bzw. Verwerten von nur den wichtigen Nachrichten wird das Sicherheitssystem von Ballast entlastet, weil nur die notwendigen Nachrichten bearbeitet werden.

[0012] Die o.g. Notastaster und Endschalter werden der Redundanz wegen mit doppelten Kontakten ausgestattet von denen der eine durch die Sicherheits Ein-/Ausgabeeinrichtung und der andere über eine separate betriebsmäßige Ein-/Ausgabeeinrichtung eingelesen wird. Es ist aber auch möglich, beide Kontakte mit derselben Sicherheits Ein-/Ausgabeeinrichtung einzulesen, jedoch über getrennte Eingänge. Die betriebsmäßig vorgesehene Ein-/Ausgabeeinrichtung meldet ihre Nachricht der eigentlichen Betriebssteuerung, welche

die entsprechenden Funktionen ausführt. Im Falle, daß die Sicherheits Ein-/Ausgabeeinrichtung beide Kontakte einliest, wird der betriebsmäßig vorgesehene Vorgang auch von der Betriebssteuerung vorgenommen. Das Sicherheitskonzept wird dadurch nicht verlassen, es wird lediglich das Einlesen durch das gleiche Hardwaremittel vorgenommen. Die Sicherheitsüberwachungssteuerung die auf die Nachricht der Sicherheits Ein-/Ausgabeeinrichtung Zugriff hat, ermittelt daraus die erlaubten Betriebszustände und wird erst aktiv, wenn ein fehlerhafter Zustand vorliegt. Ein fehlerhafter Zustand liegt beispielsweise dann vor, wenn sich ein Antrieb außerhalb der Befehlsvorgabe der Betriebssteuerung befindet. Die Redundanz liegt in der doppelten Ausführung der Kontakte der jeweiligen Schalter und Taster und der doppelten Ausführung der Ein-/Ausgabeeinrichtungen ("normale" Ein-/Ausgabeeinrichtung und Sicherheits Ein-/Ausgabeeinrichtung). Am Antrieb selbst, sind neben dem Encoder am Motor, entweder ein zusätzlicher Encoder angebracht oder der Geber am Motor gilt als sicher, der dann mit einer redundanten Auswertung versehen wird. Die in jedem Fall doppelten Signale werden der Antriebssteuerung und der Sicherheitsüberwachungssteuerung zugeführt.

[0013] Neben der oben angeführten sogenannten Hardwareredundanz gibt es weiterhin eine Redundanz in der Überwachung der Funktion. Das heißt die Sicherheitsüberwachungssteuerung ist der Betriebssteuerung als Überwachungsorgan zugeteilt. Fällt die Betriebssteuerung aus, bzw. liegt ein Fehlverhalten vor, werden sämtliche sicherheitsrelevanten Funktionen durch die Sicherheitsüberwachungssteuerung in einen sicheren Zustand geführt. Dieses ist deshalb möglich, weil sowohl die Betriebssteuerung, als auch die Sicherheitsüberwachungssteuerung über die sicherheitsrelevanten Betriebszustände gleiche Informationen haben. Der Begriff "gleiche Information" gilt solange, wie die redundante Überwachung der sicherheitsrelevanten Betriebszustände identische Ergebnisse liefert. Ist dieses nicht der Fall, tritt die Sicherheitsüberwachungssteuerung in Kraft. Ob eine Übereinstimmung der Informationen in der Betriebssteuerung und der Sicherheitsüberwachungssteuerung besteht, wird mittels eines Konsistenzchecks geprüft. Dieser Check kann in der Betriebssteuerung, oder in der Sicherheitsüberwachungssteuerung stattfinden. Falls die verschiedenen Steuerungen an separaten, mittels Buskoppler verbundenen Bussystemen hängen, kann der Konsistenzcheck auch in dem Buskoppler vorgenommen werden. Der Konsistenzcheck bringt den Vorteil, daß ein Wiederauflaufen der Maschine nach einem fehlerhaften Zustand erst dann möglich ist, wenn der Fehler behoben ist.

[0014] Welche Steuerung (die eigentliche Betriebssteuerung, oder die redundante Sicherheitsüberwachungssteuerung) letztendlich die Maßnahme bestimmt, wird folgendermaßen festgelegt:

Der Normalbetrieb wird immer durch die eigentli-

chen Betriebssteuerung vollzogen. Der Normalbetrieb liegt dann vor, wenn die Sicherheitsüberwachungssteuerung keinen fehlerhaften Zustand der Betriebssteuerung feststellt. Liegt ein fehlerhafter Zustand vor, greift die Sicherheitsüberwachungssteuerung ein und führt das Stell-/Antriebsselement entsprechend der Vorgaben in den sicheren Zustand.

[0015] Das Bussystem muß nicht redundant aufgebaut sein, es ist vielmehr erforderlich daß ein Ausfall des Bussystems sicher erkannt wird. Da die Sicherheitsüberwachungssteuerung direkt dem Antrieb zugeordnet ist und bei Ausfall des Bussystems eine in der Sicherheitsüberwachungssteuerung abgelegte Routine den Antrieb in den sicheren Zustand führt.

Das gleiche gilt für die Sicherheits Ein-/Ausgabeeinrichtung. Falls diese einen Ausfall des Bussystems erkennt, werden ebenfalls Maßnahmen ausgeführt, die einen sicheren Zustand der anzusteuern Stellen bewirken. Diese Maßnahmen sind ebenso auf der Sicherheits Ein-/Ausgabeeinrichtung hinterlegt.

[0016] Es ist jedoch denkbar, daß ein Bussystem in der Übertragungsgeschwindigkeit beeinträchtigt wird, wenn eine große Anzahl von Teilnehmern angeschlossen sind, bzw. wenn die Strecke die ein Bussystem abdeckt sehr lang ist, daß beispielsweise für den Sicherheitsweg und den Betriebsweg getrennte Bussysteme vorgesehen sind. In diesem Fall wird eine Kopplung des einen Bussystems mit dem anderen mittels einer Buskopplung durchgeführt. Denkbar ist auch, daß mehrere Bussysteme durch eine solche Buskopplung verbunden werden. Daß ein Bussystem bezüglich der Übertragungsgeschwindigkeit nicht beeinträchtigt ist, wird bei der Konzeption vermieden. Aber auch eine Beeinträchtigung der Übertragungsgeschwindigkeit des Bussystems wird erkannt und die Maschine in den sicheren Zustand beführt.

[0017] Um zu erkennen, ob ein Bussystem ausgefallen ist gibt es die Möglichkeit, daß die verschiedenen Teilnehmer sich in einem definierten Zeittakt Informationen zusenden. Bleibt eine Information aus wird dieses als Ausfall des Bussystems gewertet und die Sicherheitsüberwachungssteuerungen, für die der Ausfall des Bussystems relevant ist aktivieren die Routinen, die zum sicheren Zustand führen. Diesen Überwachungsvorgang bezeichnet man als Watch Dog. Anhand des zyklischen Sendens und Empfangens von Informationen kann beim Ausfall eines lokalen Bussystems erkannt werden welches der lokalen Bussysteme einen Defekt hat. Es ist dann auch denkbar, daß die Buskopplung eine Information auf die noch intakten Bussysteme legt, wodurch der Defekt des gestörten Bussystems gemeldet wird. Ob nun eine Sicherheitsüberwachungseinrichtung an einem noch intakten Bussystem auf diese Meldung reagiert oder nicht obliegt der Sicherheitsüberwachungseinrichtung selbst, da sie erkennt ob aus der Situation ein sicherheitskritischer Zustand entsteht oder

nicht.

[0018] Eine weitere Variante der Erfindung sieht vor, für verschiedene Betriebszustände der Maschine unterschiedliche Überwachungskriterien zu definieren. Wird eine Maschine bei offenem Schutzgitter in einem vom eigentlichen Betriebsfall abweichenden Schleichgang betrieben, werden hierzu andere Sicherheitsanforderungen gestellt, die vom Bediener durch entsprechende Eingaben definiert werden. Beispielsweise das Drücken eines separaten Schalters oder Tasters kann diesen Schleichgang einleiten. Da dieser Schleichgang sicherheitsrelevant ist und das geöffnete Schutzgitter von der Sicherheits Ein-/Ausgabeeinrichtung erkannt wird, steht eine entsprechende Nachricht der Sicherheitsüberwachungssteuerung zur Verfügung. Die Sicherheitsüberwachungssteuerung kann nun im Gegensatz zum normalen Betriebsfall, bei dem ein geöffnetes Schutzgitter zum Stillstand der Maschine führen würde, auch bei offenem Schutzgitter eine maximale Geschwindigkeit des Antriebselements zulassen. Das heißt eine Freigabe zum Betrieb des Antriebs erteilen. Unterschiedliche Überwachungskriterien können sich weiterhin auf die Überwachung der Winkelposition, die Beschleunigung, das Drehmoment oder sonstiges beziehen. Somit können den verschiedenen Betriebsarten unterschiedliche Sicherheitsbestimmungen zugeordnet werden.

[0019] Bezüglich der räumlichen Anordnung der Sicherheitsüberwachungssteuerung ist folgende Variante möglich:

Das Stell-/Antriebsselement verfügt über eine direkt ihm zugeordnete Regelung, Stromrichter und Leistungsteil. Diese Regelung empfängt seitens der Betriebssteuerung Befehle, welche beispielsweise heißen:

- fahre mit einer konstanten Drehzahl 3000 Druck/h,
- bringe das Antriebselement bei der Winkelstellung 270 Grad zum Stillstand,
- usw.

[0020] Das heißt, die Aufgabe der Betriebssteuerung besteht darin, Befehle zu verwalten und auszugeben. Die nun die Betriebssteuerung und die Antriebe überwachende Sicherheitsüberwachungssteuerung wird deshalb auch dem Stell-/Antriebsselement zugeordnet, weil im Falle eines Fehlers ein Herunterführen in den sicheren Zustand direkt am Stell-/Antriebsselement durchgeführt werden kann, auch ohne daß Befehle über das Bussystem geschickt werden müssen. In diesem Fall bringt die Sicherheitsüberwachungssteuerung über redundante Signale das Stell-/Antriebsselement in den sicheren Zustand. Die räumliche Zuordnung der Sicherheits Ein-/Ausgabeeinrichtung ist ähnlich vorgesehen. Diese wird auch unmittelbar vor Ort dort angebracht wo eine Einlesen bzw. eine Ausgabe erfolgt.

[0021] Da diese Sicherheits Ein-/Ausgabe Einrich-

tung einen universellen Aufbau mit mehreren möglicherweise frei definierbaren Ein-/Ausgängen hat, kann diese Einrichtung auch dazu benutzt werden, nichtsicherheitserlevante Ein- oder Ausgänge zu verwalten. Damit kommt der Sicherheits Ein-/Ausgabe Einrichtung eine Doppelfunktion zu. Nicht zuletzt wegen der o.g: Doppelfunktion kann das System als aufwandssparende Redundanz bezeichnet werden.

[0022] Die frei konfigurierbaren Ein-/Ausgängen der Sicherheits Ein-/Ausgabe Einrichtung bieten den Vorteil, daß diese als Module in hoher Stückzahl gefertigt werden können und deshalb kostengünstig sind.

[0023] Ein zusätzlicher Vorteil der Standardisierung ist darin zu sehen, daß der Servicetechniker vor Ort nur eine geringe Anzahl von Varianten beachten muß, daß dadurch ein schneller Austausch vorgenommen werden kann und die Verfügbarkeit der Maschine schnell wieder hergestellt ist. Es ist auch denkbar eine Sicherheits Ein-/Ausgabeeinrichtung an einer weniger oder für verschiedene Betriebsarten nicht benutzten Komponente zu entnehmen und gegen eine defekte auszutauschen. Die Konfiguration des Moduls könnte durch eine vom Betriebsrechner der Maschine vorgenommene Softwareeinspielung erfolgen. Um den Vorschriften der Berufsgenossenschaft gerecht zu werden, wäre bei diesem Vorgang eine abschließende Sicherheitsabnahme erforderlich, die beispielsweise so aussehen kann, daß bei nicht sachgemäßer Konfiguration der Sicherheits Ein-/Ausgabeeinrichtungen ein Anlaufen der Maschine verhindert wird.

[0024] In einer weiteren Variante ist vorgesehen, daß eine Maschine nicht nur aus einer Komponente besteht, sondern wie in der Druckindustrie üblich aus einer Druckmaschine die das Bebildern von Papier vornimmt und einer im Anschluß an diese Maschine befindlichen Weiterverarbeitungsmaschine, beispielsweise aus einem Falzapparat. Für sich genommen können beide Komponenten steuerungstechnisch separate Einheiten bilden, die jedoch im Sicherheitskonzept als einheitlich zu betrachten sind. Für diesen Fall ist es vorgesehen, die jeweils getrennten Bussysteme miteinander durch einen Buskoppler zu verbinden, so daß die sicherheitsrelevanten Nachrichten von den Sicherheits Ein-/Ausgabeeinrichtungen allen an den beiden Bussystemen angekoppelten Sicherheitsüberwachungssteuerungen zugänglich sind. Die Vorgehensweise bezüglich dem Umgang mit der Nachricht ist identisch mit der eingangs beschriebenen Art. Selbstverständlich ist auch eine Kopplung mehrerer Bussysteme denkbar.

[0025] Die Erfindung soll nachträglich anhand von eines Ausführungsbeispiels näher erläutert werden. Es zeigt:

Fig. 1 ein Blockschaltbild des Sicherheitskonzepts,
Fig. 2 ein Blockschaltbild des Sicherheitskonzepts mit getrennten Bussystemen.

[0026] Fig. 1 zeigt eine Betriebssteuerung 1 für eine

Anzahl von Antriebs und Stellvorgängen an einer nicht dargestellten Maschine, vorzugsweise Druckmaschine. Diese Betriebssteuerung 1 ist mittels Bussystem 2 mit einer Anzahl von Ein-/Ausgabeeinrichtungen 3, mit Sicherheits Ein-/Ausgabeeinrichtungen 4, mit einer Antriebssteuerung 5 und einer Sicherheitsüberwachungssteuerung 6 verbunden. Die Aufgabe der Betriebssteuerung 1 besteht darin die Koordination der verschiedenen Antriebe 7, welche den Hauptantrieb der Maschine, Hilfsantriebe für verschiedene Aufgaben wie z.B. Heben und Senken des Papierstapels, Antreiben des Farbdukts oder ähnliches und auch Stellantriebe beispielsweise zum Verstellen von Registern betrifft. Zusätzlich werden durch die Betriebssteuerung 1 auch das Zusammenspiel von Stellelementen 8 das Einlesen von Schaltern 9, 10 oder die Anzeigen 11 koordiniert. Als Ein-/Ausgabeeinrichtungen dienen dazu die Ein-/Ausgabeeinrichtungen 3 und die Antriebssteuerung 5. Den sicherheitsrelevanten Stellvorgängen ist eine Sicherheits Ein-/Ausgabeeinrichtung 4 zugeordnet, welche redundant diese Vorgänge steuert, bzw. einliest.

[0027] Der Antrieb 7, welcher wie bereits erwähnt ein Hauptantrieb, ein Hilfsantrieb oder auch ein Stellantrieb sein kann, die wiederum durch Motoren verschiedenster Technologien (Gleichstrommotor, Drehstrommotor, bürstenloser Motor etc.) ausgeführt sein können, wird durch die Antriebssteuerung 5 mittels Leistungsteil 12 in Betrieb gesetzt. Die Verbindung zwischen Antriebssteuerung 5 und Leistungsteil 12 ist bidirektional. Auf das Leistungsteil 12 hat auch die Sicherheits Ein-/Ausgabeeinrichtung 4 bidirektionalen Zugriff. An dem Antrieb 7 befinden sich je ein Encoder 13, 14 welcher aus einem Geber und einer Auswerteschaltung besteht, wodurch die Position, möglicherweise auch die Drehzahl des Antriebs 7 erfaßt wird. Diese Information wird von beiden Encodern 13, 14 einerseits der Antriebssteuerung 5 und andererseits der Sicherheits Ein-/Ausgabeeinrichtung 4 zugeleitet. Weiterhin besteht jeweils von der Antriebssteuerung 5 und der Sicherheits Ein-/Ausgabeeinrichtung eine Ansteuermöglichkeit zu einer Bremse 15, die in mechanischer Wirkverbindung zu dem Antrieb 7 steht und diesen im Notfall stillsetzen kann. Tritt ein fehlerhaftes Verhalten der Antriebssteuerung 5 ein, wodurch der Antrieb 7 außerhalb der vorgegebenen Drehzahl betrieben wird, greift die Sicherheitsüberwachungseinrichtung 6 direkt auf das Leistungsteil 12 zu, unterbricht die Stromzufuhr für den Antrieb 7 und läßt die Bremse 15 einfallen. Der Antrieb 7 ist somit in den sicheren Zustand geführt.

[0028] Das Stellelement 8, welcher beispielsweise ein Pneumatikzylinder zum An- und Abstellen von Farbwalzen sein kann, wird durch eine Ein-/Ausgabesteuerung 3 aktiviert. Redundant dazu ist der Zugriff auch über eine Sicherheits Ein-/Ausgabeeinrichtung vorgesehen. Falls hier ein fehlerhaftes Verhalten vorliegt, bringt die Sicherheits Ein-/Ausgabeeinrichtung den Stellelement 8 in den sicheren Zustand.

[0029] Die Schalter 9, 10 sind sicherheitsrelevant,

weil sie z.B. einen Notstop auslösen, oder den geöffneten Zustand eines Schutzgitters darstellen. Beide Zustandsabfragen werden als sicherheitsrelevante Eingaben bezeichnet, weshalb redundante Schalterkontakte 9a, 9b und 10a, 10b erforderlich sind. Diese werden auf getrenntem Weg durch die Ein-/Ausgabeeinrichtung 3 und die Sicherheits Ein-/Ausgabeeinrichtung 4 eingelesen. Die Sicherheits Ein-/Ausgabeeinrichtung 4 kann für alle Anwendungsfälle eine gemeinsame Einrichtung oder für jeden Anwendungsfall getrennt vorhanden sein. Dieses ist abhängig von der Anzahl der zur Verfügung stehenden Ein-/Ausgänge bzw. von der räumlichen Zuordnung. Bei fehlerloser Funktion der Schalter 9,10 haben die Schalterkontakte 9a,9b und 10a, 10b jeweils gleiche Zustände. Ist ein Schalterkontakt 9a,9b oder 10a,10b fehlerhaft oder ist die Kabelverbindung zwischen Schalterkontakt 9a,9b oder 10a, 10b fehlerhaft, werden in der Ein-/Ausgabeeinrichtung 3 und der Sicherheits Ein-/Ausgabeeinrichtung 4 unterschiedliche Zustände erkannt. Die Sicherheitsüberwachungseinrichtung 6 bringt daraufhin den Antrieb 7 und den Stellelement 8 in den sicheren Zustand.

[0030] Durch die Betriebssteuerung 1 kann auch ein Zugriff auf Ein- oder Ausgänge erfolgen die durch die Sicherheits Ein-/Ausgabeeinrichtung 4 bedient werden. Diese Ein- oder Ausgänge sind dann als gewöhnliche Ein- oder Ausgänge definiert, das heißt sie werden nicht als sicherheitsrelevant betrachtet. Der Vorteil besteht darin, daß freie, nicht benutzte Ein- oder Ausgänge auf der Sicherheits Ein-/Ausgabeeinrichtung genutzt werden können. Diese sind zum Beispiel für die Anzeige 16 oder ähnliche Funktionen verwendbar.

[0031] Fig. 2 zeigt im wesentlichen die gleiche Anordnung der Sicherheitseinrichtungen wie Fig. 1 jedoch mit getrennt aufgebauten Bussystemen. Hierbei wird das Bussystem 2 für die Anbindung der Sicherheits Ein-/Ausgabeeinrichtung 4 und der Sicherheitsüberwachungseinrichtung 6 benutzt, während ein zusätzliches Bussystem 17 die Anbindung der eigentlichen Betriebs-einrichtungen Ein-/Ausgabeeinrichtung 3 und Antriebssteuerung 5 übernimmt. Diese Konstellation ist dann vorteilhaft, wenn eine hohe Anzahl von Busteilnehmern (3,4,5,6) an dem Bussystem hängt oder wenn die Leitungslänge des Bussystems eine bestimmte Länge überschreitet. In Fig. 2 werden die Bussysteme 2, 17 durch einen Buskoppler 18 gekoppelt. Es ist erkennbar, daß durch den Buskoppler 18 noch weitere Bussysteme 19 angebunden werden können. Die Betriebssteuerung 1 ist durch ein weiteres Bussystem 20, welches beispielsweise ein VME-Bussystem sein kann, mit dem Buskoppler 18 verbunden.

Bezugszeichenliste

[0032]

- | | |
|---|-------------------|
| 1 | Betriebssteuerung |
| 2 | Bussystem |

- | | |
|----------|---|
| 3 | Ein-/Ausgabeeinrichtung (Busteilnehmer) |
| 4 | Sicherheits Ein-/Ausgabeeinrichtung (Busteilnehmer) |
| 5 | Antriebssteuerung (Busteilnehmer) |
| 6 | Sicherheitsüberwachungseinrichtung (Busteilnehmer) |
| 7 | Antrieb |
| 8 | Stellelement |
| 9 | Schalter |
| 9a,9b | Schalterkontakt |
| 10 | Schalter |
| 10a, 10b | Schalterkontakt |
| 11 | Anzeige |
| 12 | Leistungsteil |
| 13 | Encoder |
| 14 | Encoder |
| 15 | Bremse |
| 16 | Anzeige |
| 17 | Bussystem |
| 18 | Buskoppler |
| 19 | Bussystem |
| 20 | Bussystem |

25 Patentansprüche

1. Vorrichtung zur Überwachung von sicherheitsrelevanten Vorgängen an Stell-/ Antriebselementen an einer Maschine insbesondere Druckmaschine mit einer Betriebssteuerung für eine Anzahl von Antriebs- und Stellvorgänge und mindestens einer mit einer Anzahl von Sicherheits Ein-/Ausgabeeinrichtungen in Verbindung stehenden Sicherheitsüberwachungssteuerung
dadurch gekennzeichnet,
dass die Signale der Stell-/ Antriebselemente durch die Sicherheits Ein-/Ausgabeeinrichtung (4) einlesbar sind, dass ein Bussystem (2) zur Übermittlung der Signale zu der Sicherheitsüberwachungssteuerung (6) vorgesehen ist,
und **dass** die Stell-/ Antriebselemente beim Erkennen eines fehlerhaften Zustandes durch die Sicherheitsüberwachungssteuerung (6) mittels der Sicherheits Ein-/Ausgabeeinrichtung (4) in den sicheren Zustand bringbar sind.
2. Vorrichtung nach Anspruch 1,
dadurch gekennzeichnet,
dass das Bussystem (2) als VME-Bussystem ausgeführt ist.
3. Vorrichtung nach Anspruch 1,
dadurch gekennzeichnet,
dass das Bussystem (2) mehrere Sicherheits Ein-/Ausgabeeinrichtungen (4) mit einer oder mehreren für einen sicherheitskritischen Bereich verantwortlichen Sicherheitsüberwachungssteuerungen (6) verbindet.

4. Vorrichtung nach Anspruch 1,
dadurch gekennzeichnet,
dass die Sicherheitsüberwachungssteuerung (6)
als Modulbauweise konzipiert ist. 5
5. Verfahren zur Überwachung von sicherheitsrele-
vanten Vorgängen an Stell-/Antriebselementen an
einer Maschine, vorzugsweise Druckmaschine,
dadurch gekennzeichnet,
dass von einer Sicherheits Ein-/Ausgabeeinrich- 10
tung (4) Signale von den sicherheitsrelevanten Vor-
gängen dezentral eingelesen und mittels Bussy-
stem (2) einer Sicherheitsüberwachungssteuerung
(6) zugeführt werden,
dass bei Erkennen eines sicherheitsrelevanten Zu- 15
standes entsprechende Maßnahmen mittels des
Bussystems (2) der Sicherheits Ein-/Ausgabeein-
richtung (4) zugeführt und dort ausgeführt werden.
6. Verfahren nach Anspruch 5, 20
dadurch gekennzeichnet,
dass die Sicherheits Ein-/Ausgabeeinrichtung (4)
entsprechend einem Broadcast-Verfahren ihren
eingelesenen Zustand auf das Bussystem (2) legt. 25
7. Verfahren nach Anspruch 5,
dadurch gekennzeichnet,
dass zur Überprüfung des Bussystems (2) von den
verschiedenen Busteilnehmern (3,4,5,6,) in einem
definierten Zeittakt Informationen zugesendet wer- 30
den.
8. Verfahren nach Anspruch 7,
dadurch gekennzeichnet,
dass bei Ausfall des Bussystems (2) eine in der Si- 35
cherheits Ein-/Ausgabeeinrichtung (4) abgelegte
Routine das Stell-/Antriebselement in den sicheren
Zustand führt.

40

45

50

55

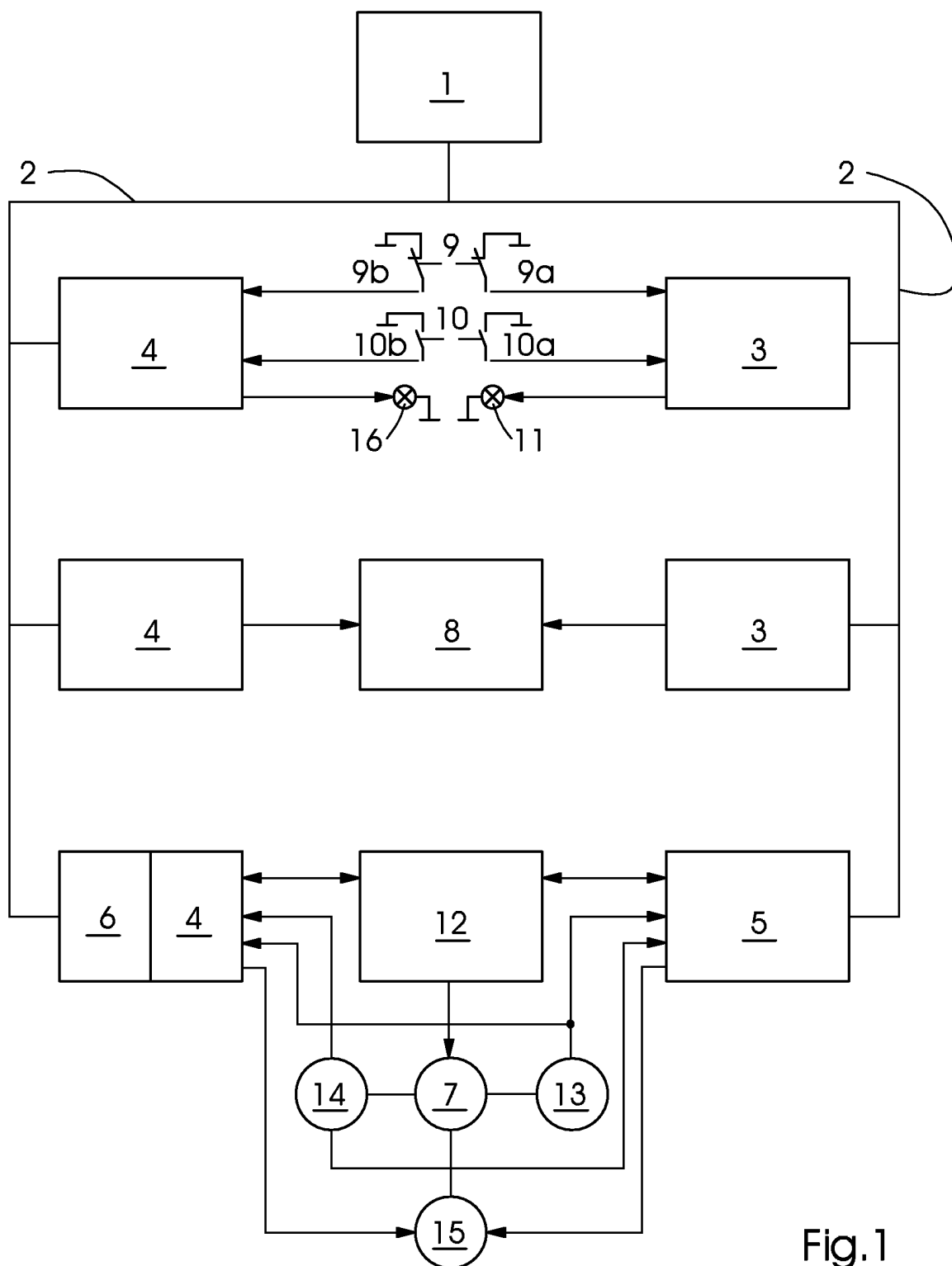


Fig.1

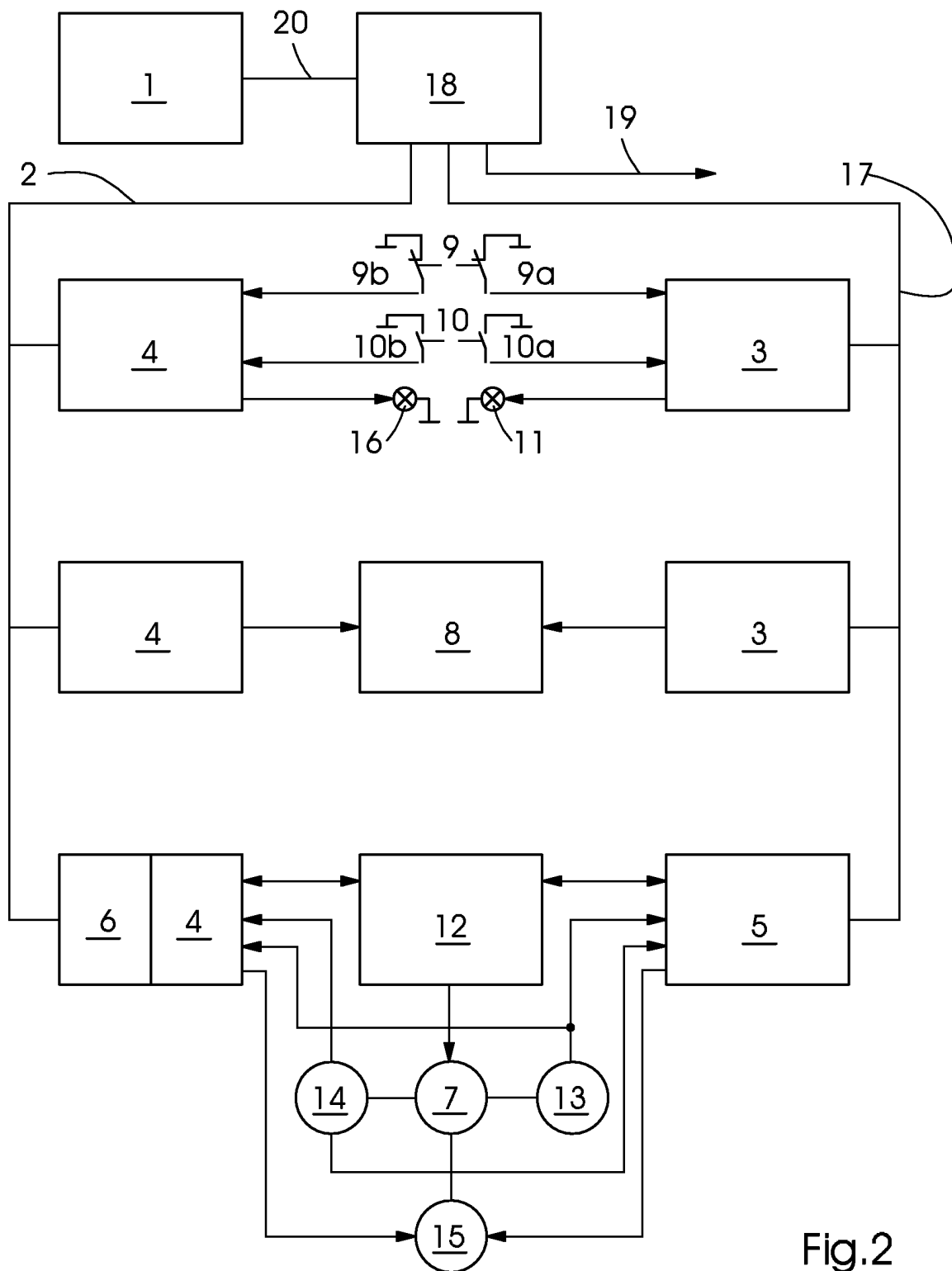


Fig.2