

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
27. April 2006 (27.04.2006)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2006/042775 A2

(51) Internationale Patentklassifikation:
Nicht klassifiziert

TEGELER, Jürgen [DE/DE]; Auf der Leiten 2, 82377 Penzberg (DE).

(21) Internationales Aktenzeichen: PCT/EP2005/054609

(74) Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, 80506 München (DE).

(22) Internationales Anmeldedatum:
16. September 2005 (16.09.2005)

(81) Bestimmungsstaaten (soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2004 050 350.8
15. Oktober 2004 (15.10.2004) DE

(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(84) Bestimmungsstaaten (soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU,

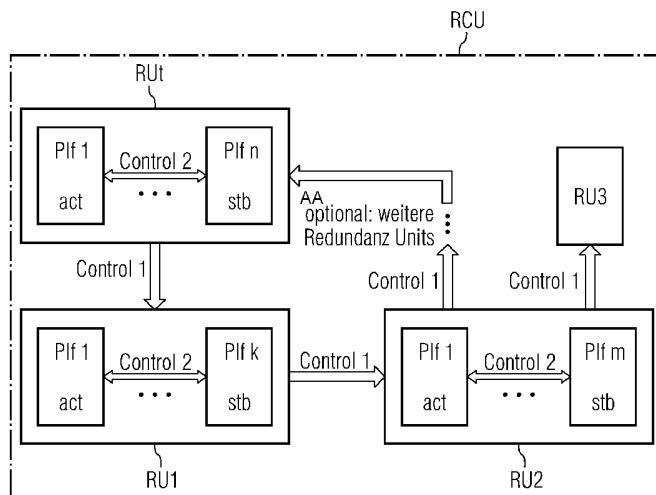
(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): LÖBIG, Norbert [DE/DE]; Im Erlich 79, 64291 Darmstadt (DE).

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND DEVICE FOR REDUNDANCY CONTROL OF ELECTRICAL DEVICES

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR REDUNDANZKONTROLLE VON ELEKTRISCHEN EINRICHTUNGEN



AA ... OPTIONAL: ADDITIONAL REDUNDANCY UNITS

(57) Abstract: In general, electrical units have to meet the requirements for high reliability and a high level of operational safety. This applies in particular to communications systems where the constant availability of all devices is necessarily required. For this reason, computer capacity is held in reserve in order to guarantee operational safety, so that in the event of failure of an electrical device, the currently-running functions can be transferred to additional (active) electrical devices. The control of these processes is carried out by a redundancy control. However, the problem associated with prior art remains, whereby all processes for redundancy control are expensive (additional hardware/devices) or unreliable (risk of split-brain), sometimes even both. The invention provides a solution by virtue of the fact that each of the electrical devices is monitored by an additional electrical device and that, optionally, each of these devices, in turn, monitors at least one of the electrical devices.

[Fortsetzung auf der nächsten Seite]

WO 2006/042775 A2



TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Veröffentlicht:

- ohne internationalen Rechenbericht und erneut zu veröffentlichen nach Erhalt des Berichts

(57) Zusammenfassung: Von elektrischen Einrichtungen wird in der Regel eine hohe Zuverlässigkeit und Betriebssicherheit gefordert. Dies gilt insbesondere für Kommunikations Systeme, wo die ständige Verfügbarkeit aller Einrichtungen zwingend erforderlich ist. Aus diesem Grund wird zur Sicherstellung der Betriebssicherheit Rechnerkapazität in Reserve gehalten, um bei Ausfall einer elektrischen Einrichtung die hier momentan ablaufenden Funktionen auf (aktive) weitere elektrische Einrichtung übertragen zu können. Die Steuerung dieser Vorgänge wird von einer Redundanzkontrolle übernommen. Problematisch bei dem Stand der Technik ist, dass alle Verfahren zur Redundanzkontrolle teuer (zusätzliche HW/Einrichtungen) oder unzuverlässig (Gefahr von Split Brain) oder manchmal auch beides sind. Die Erfindung schafft hier Abhilfe, indem vorgesehen ist, dass jede der elektrischen Einrichtungen von einer weiteren der elektrischen Einrichtungen überwacht wird, und ggf. ihrerseits wenigstens eine der elektrischen Einrichtungen überwacht.

Beschreibung

Verfahren und Vorrichtung zur Redundanzkontrolle von elektrischen Einrichtungen

5

Von elektrischen Einrichtungen wird in der Regel eine hohe Zuverlässigkeit und Betriebssicherheit gefordert. Dies gilt insbesondere für Kommunikationssysteme, wo die ständige Verfügbarkeit aller Einrichtungen zwingend erforderlich ist (Hochverfügbarkeit). Aus diesem Grund wird im Kommunikationssystem zur Sicherstellung der Betriebssicherheit Rechnerkapazität in Reserve gehalten, um bei Ausfall einer elektrischen Einrichtung die hier momentan ablaufenden Funktionen auf (aktive) weitere elektrische Einrichtung übertragen zu können. Sind letztere auf einen solchen Fall bereits derart vorbereitet, dass sie die Funktionen unmittelbar übernehmen können ohne z. B. umkonfiguriert oder neu installiert werden zu müssen, spricht man von Redundanz. Um bei Ausfall elektrischer Einrichtungen deren Funktionen schnell, sicher und nachvollziehbar auf andere elektrischen Einrichtungen übertragen zu können, ist eine Redundanzkontrolle erforderlich. Deren Aufgabe besteht darin, regelmäßig den Zustand aller elektrischen Einrichtungen zu prüfen, um bereits im Vorfeld eines möglichen Ausfalls den aktuellen Betriebszustand aller elektrischen Einrichtungen zu kennen, um bei Ausfall einer Einrichtung das Umschalten der Funktionen effektiv steuern zu können.

Grundsätzlich werden beim Stand der Technik für redundante Systeme zwei Architekturen unterschieden:

(i) So wird zum einen eine Mehrzahl von Einrichtungen vorgesehen, die aus Sicht der Applikation, für die sie Redundanz zur Verfügung stellen, völlig homogen sind. Damit ist ein Ressourcen-Pool mit einer Mehrzahl von Einrichtungen definiert, der im Fehlerfall den auf einer fehlerbehafteten elektrischen Einrichtung ablaufenden Applikationen Ressourcen

auf funktionierenden Einrichtungen zuweist (z. B. MGCP Protokoll, Code Receiver, Echo Cancellor). Wenn die fehlerhafte Einrichtung wieder in Betrieb geht, wird sie wieder in den Ressourcen-Pool zurückgegeben und steht den Applikationen
5 wieder zur Verfügung. Die zwischenzeitlich benutzten Ressourcen auf den anderen Einrichtungen sind dann wieder frei.

(ii) Zum anderen existieren Konfigurationen, in denen zumindest gewisse Applikationen im Block von einer elektrischen
10 Einrichtung bei Ausfall derselben auf eine andere elektrischen Einrichtung migriert werden (z. B. H.248 Protokoll). Diese ist zur Übernahme der Funktion ausgezeichnet bzw. z.B. durch ständig aktualisierte Datenvorbereitet worden, wobei nur hierdurch die prinzipielle und schnelle Übernahme der
15 Funktion ermöglicht wird. Auswahl der redundanten Einheit aus einem Pool genügt in diesem Falle nicht, da die Vorbereitung zu komplex und langwierig wäre, was unerwünschte Auswirkung auf die geforderte Verfügbarkeit der Funktion hätte.

20 Während für (i) sich leicht effiziente und sichere Verfahren der Redundanzkontrolle realisieren lassen, haben die bekannten Verfahren der Redundanzkontrolle im Fall (ii) einige gravierende Nachteile. Hier ist in der Regel ein zusätzlicher Controller erforderlich, um die redundanten elektrischen Ein-
25 richtungen zu überwachen und im Falle des Ausfalls die Ersatzschaltung durchzuführen. Um Hochverfügbarkeitsanforderungen wirklich gerecht werden zu können, muss zudem der Controller in sich selbst auch redundant sein. Hierfür muss ebenfalls ein Redundanzmechanismus existieren. Erst mit diesem
30 Aufwand ist die Redundanzkontrolle sicher und erfüllt damit zumindest in den meisten Fällen Echtzeitanforderungen. Derartige Systeme sind aber sehr teuer.

35 Gemäß einem weiteren Stand der Technik ist vorgesehen, dass zwei elektrische Einrichtungen sich permanent gegenseitig überwachen. Hierzu wird eine der elektrischen Einrichtungen in

einen aktiven Betriebszustand (act) gesteuert, während die verbleibende elektrische Einrichtung in einem bereitstehenden oder Standby-Betriebszustand (stb) verbleibt. Dabei sind alle Applikationen der sich im Standby-Betriebszustand befindlichen elektrischen Einrichtungen deaktiviert. Gelangt nun
5 letztere zu dem Schluss, dass die aktive elektrische Einrichtung ausgefallen ist, steuert sie sich selbst in einen aktiven Betriebszustand.

10 Dieses Verfahren birgt ein relativ großes Risiko, dass das sogenannte "Split Brain" Szenario auftritt. Beim "Split Brain" Szenario gleichen beide Redundanz Partner ihre Betriebszustände nicht mehr konsistent zueinander ab. Dies bedeutet, dass sich beide Partner im Standby oder aktiven Betriebszustand befinden können. Es kann auch ein synchrones
15 Schwingen beider Systeme zwischen aktivem und Standby-Betriebszustand auftreten. Unter Umständen ist ein solcher Zustand nur manuell behebbar. Die Auswirkungen eines solchen Szenarios sind verheerend für den Betrieb. Das Risiko des Auftretens von "Split Brain" sollte daher bei der Auswahl eines hochzuverlässigen Redundanzverfahrens vermieden werden.
20

Diese Gefahr kann zwar konzeptionell bereits reduziert werden, indem die Entscheidung über (act/stb) zwischen zwei Redundanz Partnern von einer dritten, neutralen Einheit getroffen wird, die dann allen betroffenen elektrischen Einrichtungen ihre Entscheidung mitteilt und sie dazu zwingt, einen bestimmten Zustand anzunehmen. Eine derartige Lösung ist bereits für Kommunikationssysteme vorgeschlagen worden. Hierbei
25 übernimmt die hochverfügbare zentrale Steuervorrichtung die Funktion der Redundanzkontrolle über die peripheren elektrischen Einrichtungen. Damit ist dann aber wieder die eingangs geschilderte (teuere) Konfiguration gegeben. Grundsätzlich kann der Stand der Technik als teuer oder unzuverlässig
30 (manchmal auch beides) bezeichnet werden.
35

Der Erfindung liegt daher die Aufgabe zugrunde, einen Weg aufzuzeigen und eine Vorrichtung anzugeben, die für elektrische Einrichtungen eine effiziente und kostengünstige Methode zur Redundanzkontrolle darstellen.

5

Die Erfindung wird ausgehend von dem im Oberbegriff der Patentansprüche 1 und 10 angegebenen Merkmalen durch die kennzeichnenden Merkmale gelöst.

10 Der Vorteil an der Erfindung liegt in der Bereitstellung eines einfachen und effizienten Redundanzmechanismus, der für die Redundanzkontrolle keine zusätzliche Hardware benötigt, und zugleich ein Maximum an Verfügbarkeit und Betriebssicherheit gewährt. Dies wird durch das Vorsehen einer zwei-
15 stufigen Redundanzkontrolle erreicht, wobei die erste Stufe (Control 1) über eine neutrale, dritte Instanz verfügt, die über die Ersatzschaltung innerhalb eines Redundanzpaares (Redundanz Unit) entscheidet. Dieses Konzept verringert die Gefahr von Split Brain erheblich. Das kontrollierende Paar ist
20 dabei gleichzeitig auch kontrolliertes Paar nach demselben Mechanismus. Es gibt also keinen separaten Mechanismus für die Ersatzschaltung des Kontrollierers. Damit ist die Redundanzkontrolle denkbar einfach und effizient. Alle Plattformen der Redundanzsteuereinheit können mit Applikationen geladen
25 werden, die eine Redundanzkontrolle verlangen. Damit ist keine Zusatzhardware erforderlich. Ein und dasselbe Verfahren macht sowohl die Kontrollierende als auch die kontrollierte Einheit hochverfügbar.

30 Ferner ist optional eine zweite Stufe (Control 2) vorgesehen, die die Kontrolle innerhalb einer Redundanzeinheit beschreibt. Sie kann zusätzlich zur ersten Stufe vorgesehen werden. Die Kombination von beiden Stufen hat den Vorteil einer besonders robusten Redundanz Konfiguration, die auch ge-
35 wisse Mehrfachausfälle von elektrischen Einrichtungen innerhalb des Quadrupels übersteht. In der Praxis bedeutet dies, dass wann immer zu einer ersatzschaltbaren Funktion noch eine

funktionsfähige Plattform existiert, diese die zugehörigen Services weiterführt.

Vorteilhaft ist ebenso, dass eventuelle negative Rückwirkungen auf das System nicht erfolgen. So entsteht ein einfaches Handling beim Hochfahren des Systems aus kontrollierender und kontrollierter Einheit. Hierzu kann man die Plattformen in beliebiger Reihenfolge hochfahren. Das System ist arbeitsfähig, sobald die erste Plattform "act" ist. In jeder beliebigen Kombination von funktionsfähigen und ausgefallenen Plattformen befindet sich das System im Zustand maximaler Redundanz und maximaler Funktionsverfügbarkeit.

Weiterhin ist besonders vorteilhaft, dass die Redundanz Handling von Funktionen bzw. Prozessen unterstützt wird, die in einer bestimmten Ausprägung (z.B. mit einer bestimmten Peripherie in Beziehung) nur jeweils auf einer Plattform zur gleichen Zeit laufen bzw. laufen dürfen (z.B. H.248, wo der gleichzeitige Zugriff verschiedener MGCs auf einen (im Sinne des H.248.1 Standards virtuellen) MG nicht zulässig ist), die aber hochverfügbar sein müssen. Dies schließt act/act Redundanz, act/stb Redundanz sowie auch n+m Redundanz mit ein. Funktionen bzw. Prozesse, die diese Einschränkung nicht haben (z.B. MGCP, wo der gleichzeitige Zugriff verschiedener MGCs auf ein einziges Port eines MGCP gesteuerten MGs per Standardisierung zulässig ist), können auf der Redundanzeinheit in Serverfarm Architektur betrieben werden. Für sie ist die Einführung des Verfahrens völlig transparent. Dies bedeutet, dass die Anwendung des Verfahrens keine Rückwirkung auf Funktionen hat, die es nicht benötigen, und damit auch in existierende Systeme leicht eingeführt werden kann.

Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen angegeben.

35

Die Erfindung wird im Folgenden anhand eines figürlich dargestellten Ausführungsbeispiels näher erläutert.

Es zeigen:

5 Fig 1 eine Redundanzsteuereinheit RCU mit t Redundanzeinheiten RU_1, RU_2, RU_3, RU_t ,

10 Fig 2 die Verhältnisse in einem Kommunikationssystem, bestehend aus einem Server Farm Controller mit paarweise angeordneten Servern (Plattformen) einer Mehrzahl von Redundanzeinheiten,

15 Fig 3 ein Fallbeispiel, demgemäß eine übergeordnete Einrichtung (Server Farm Controller SFC) keinerlei Kenntnisse über den Betriebszustand der einzelnen Plattformen (Server) einer Mehrzahl von Redundanzeinheiten hat,

20 Fig. 1 zeigt eine Redundanzsteuereinheit RCU (Redundanz Control Unit) mit beispielhaft 4 Redundanzeinheiten RU_1, RU_2, RU_3, RU_t (Redundanz Unit). Hierbei weist eine Redundanzeinheit eine Mehrzahl von elektrischen Einrichtungen auf, die bei vorliegendem Ausführungsbeispiel als HW/SW Plattformen ausgebildet sind. Jede Redundanzeinheit kann eine sich von den anderen Redundanzeinheiten unterscheidende Anzahl k, l, m, n von Plattformen aufweisen. Die Plattformen haben die Eigenschaft, dass jede auf einer Plattform der Redundanzeinheit ablaufende Funktion/ Applikation von jeder anderen Plattform der Redundanzeinheit übernommen werden kann.

30 Fig. 1 zeigt eine Konfiguration in einer allgemeinen Form. Hier wird eine Ringtopologie von Redundanz Units dargestellt (jede RU überwacht ihren Nachfolger und wird selbst von ihrem Vorgänger überwacht. Für das Funktionieren des Mechanismus ist es aber gar nicht erforderlich, dass jede RU Überwacher und Überwachter ist. Notwendig ist nur, dass jede RU von einer anderen überwacht wird. D.h. eine RU kann mehrere andere
35 RUs überwachen, aber jede RU der RCU wird von genau einer an-

deren RU überwacht. Damit sind auch quasi sternförmige Topologien denkbar (z.B.: RU1 überwacht RU2, RU3 und RU4. RU2 überwacht RU1). Im einfachsten Fall wird die Anzahl der Plattformen innerhalb einer Redundanzeinheit $k = l = m = n =$
5 2 sein. Damit ist ein (Plattform) Redundanzpaar pro Redundanzeinheit gegeben. Ebenso wird im einfachsten Fall eine Redundanzsteuereinheit RCU mit lediglich zwei Redundanzeinheiten vorgesehen sein. Damit ist die Redundanzsteuereinheit RCU aus zwei Redundanzeinheiten gebildet und diese wiederum je-
10 weils aus zwei Plattformen, womit ein Quadrupel definiert ist. Auf den Plattformen eines Redundanzpaares werden unterscheidbare Zustände geführt, im Folgenden als act (aktiver Betriebszustand) und stb (bereitstehende oder Standby-Betriebszustand) bezeichnet. Eine Applikation, die eine Redundanzkontrolle benötigt kann diese Zustände als Indikator
15 zur Steuerung ihrer Redundanz Funktion hernehmen.

Die in Fig. 1 dargestellte Redundanzsteuereinheit RCU stellt eine zweistufige Redundanzsteuerung/ Redundanzüberwachung
20 dar. Stufe 1 wird durch eine Kontrollfunktion Control 1 und Stufe 2 durch eine Kontrollfunktion Control 2 repräsentiert. Die gesamte Funktionalität wird durch die beiden Kontrollfunktionen Control 1 und Control 2 gebildet und stellt die Redundanzkontrolle dar.

25 In Stufe 1 überwachen sich die Redundanzeinheiten gegenseitig. Die Überwachung erfolgt derart, dass jede Redundanzeinheit maximal von einer anderen Redundanzeinheit überwacht wird und ihrerseits keine, eine oder mehrere Redundanzeinheiten
30 überwacht. In dem Spezialfall eines Quadrupels kontrolliert damit jedes Redundanzpaar den Fail Over im Partner Redundanzpaar der Redundanzsteuereinheit RCU und ist damit sowohl Kontrollierer als auch Kontrollierter. Der Kontrollierer überwacht und bestimmt die Zustände aller Plattformen innerhalb des kontrollierten Redundanzpaares. Er hat damit auch
35 die Aufgabe, für Konsistenz hinsichtlich der Redundanz (d.h. jeweils nur eine Plattform in "act") innerhalb des Redundanz-

paares zu sorgen. Die Kontrolle erfolgt durch regelmäßige Prüfung der Kommunikationsbeziehung zum zugeordneten Redundanzpaar. Wenn der Kontrollierer feststellt, dass die Kommunikation zu einer Plattform im Zustand "act" eine gewisse
5 Zeitdauer gestört ist, versucht er, diese zu deaktivieren, d.h. ihr den Zustand "stb" zu geben, und aktiviert ihren Redundanz Partner (durch Eintrag des Zustandes "act").

Zur Realisierung dieser Funktion werden Kontrollnachrichten
10 vorgesehen. Diese werden über die Kontrollfunktion Control 1 wenigstens von der sich im aktiven Betriebszustand befindlichen Plattform im überwachenden Redundanzpaar gesendet. Die Kontrollnachrichten enthalten optional Parameter wie z. B. "goto act/stb", mittels dem sie dem Empfänger mitteilen, dass
15 er in den aktiven oder Standby-Betriebszustand gehen soll. Dieser Parameter wird immer dann gesetzt, wenn der Sender die Information hat, welche der beiden Plattformen "act" und welche "stb" sein soll. Die Quittungen auf Kontrollnachrichten enthalten den Zustand der kontrollierten Plattformen (act/
20 stb).

Bei Doppelausfall des überwachten Redundanzpaares oder nachdem der Kontrollierer ein Recovery durchlaufen hat, hat dieser keinerlei Information über den Betriebszustand der kontrollierten Redundanzeinheit. In diesem Fall hat der Kontrollierer zwei Möglichkeiten, den überwachten Plattformen (act/
25 stb) Zustände zuzuweisen. Entweder entnimmt er die betreffenden Informationen aus ihren Quittungen und übernimmt sie. Alternativ hierzu weist er der ersten Plattform, die (wieder)
30 quittiert, den aktiven Betriebszustand zu. Dadurch dass der Parameter "go to act/ stb" immer dann gesetzt ist, wenn er gesetzt sein kann, erreicht man maximale Sicherheit.

Sollte trotz aller Vorsichtsmassnahmen doch einmal der Fall des Split Brain auftreten (d.h. beide kontrollierten Plattformen in act oder beide in stb), so erfährt der Kontrollierer das in der Quittung und kann sofort durch eine Überwachungsnachricht mit "go to act" / "go to stb" korrigieren. Da

die Frequenz der Überwachungsnachrichten (je nach Performance und Auslastung der Plattformen und Nachrichtenwege) möglichst hoch gewählt werden sollte (z.B. 10/s), würde ein Split Brain Szenario so sehr schnell korrigiert, was ein weiterer Vorteil
5 der Erfindung ist.

Stufe 2 beschreibt die Kontrolle innerhalb einer Redundanz-
einheit. Sie kann zusätzlich zur Kontrollfunktion Control 1
vorgesehen werden und sorgt für konsistente (act/stb) Zustän-
10 de innerhalb einer überwachten Redundanzeinheit (d.h. es darf
nur eine Plattform aktiv sein), wenn Control 1 ausgefallen
ist. Dies geschieht durch eine interne, gegenseitige Überwa-
chung der Plattformen, deren Ergebnisse ebenfalls zur Steue-
rung der Redundanz Zustände (act/stb) der Plattformen der Re-
15 dundanzeinheit hergenommen werden. Control 2 arbeitet autonom
und ist damit in der Lage, auch bei ausgefallener Kontroll-
funktion Control 1 noch eine Ersatzschaltfunktion innerhalb
des Redundanzpaares zur Verfügung stellen.

Umgekehrt können die Resultate von Control 2 vorzugsweise nur
20 dann ausgewertet werden, wenn Control 1 ausgefallen ist. D.h.
immer dann, wenn Control 1 aktiv ist, hat sie in diesem Falle
auch die Redundanzkontrolle. Control 2 läuft ständig mit und
übernimmt sofort die Kontrolle, wenn Control 1 ausfällt.

Durch klare Trennung der Verantwortlichkeiten kann eine ein-
25 fache Software Struktur erreicht und die Gefahr eines Kompe-
tenzkonflikts zwischen Control 1 und Control 2 vermieden wer-
den. Control 2 braucht lediglich auf der überwachten Redun-
danzeinheit aktiv zu sein. Die im Rahmen von Control 1 und
Control 2 ausgetauschten Nachrichten können neben den Ein-
30 stellinformationen bzgl. der alternativ zu schaltenden Funk-
tionen (ACT/STB) auch weitere Informationen wie z. B. Verfüg-
barkeit der Kommunikation der adressierten Plattform zu den
weiteren Plattformen ihrer Redundanzeinheit oder der kontrol-
lierenden Redundanzeinheit umfassen. Dies erhöht die Sicher-
35 heit der Redundanzsteuerung und vermeidet unnötige Schaltope-
rationen, z. B. in dem Fall, in dem die aktive Plattform
kurzzeitig nicht erreicht wird von der kontrollierenden

Plattform, aber eine STB Plattform der kontrollierten Redundanzeinheit erreichbar ist und vermeldet, dass sie selbst Kommunikation zur aktiven Plattform hat.

Die Quittungen auf Kontrollnachrichten können auch noch andere Informationen enthalten, die für die Entscheidung des Kontrollierers, welche Plattform act und welche stb sein soll, relevant sind. Z.B. kann ein relevantes Kriterium sein, ob die Plattformen der RU Kontakt haben zu anderen Einheiten des Gesamtsystems. Hat die stb Plattform hier einen besseren Verbindungsstatus, könnte das ein Grund zum Umschalten sein.

Im Falle von in einer Redundanzeinheit paarweise angeordneter Plattformen ist die Kontrollfunktion Control 2 innerhalb des Redundanzpaares so realisiert, dass nur die aktive Plattform regelmäßig Kontrollkommandos an ihren Redundanz Partner sendet. Die aktive Plattform überwacht, ob ihre Kontrollnachrichten quittiert werden. Beide Plattformen des Redundanzpaares überwachen, ob sie Kontrollkommandos vom Redundanz Partner empfangen. Mit Hilfe der Kontrollfunktion Control 2 verschafft sich jede Plattform des Redundanzpaares Informationen darüber, ob ihre Partner Plattform überhaupt mit ihr kommuniziert und falls dies der Fall ist, in welchem Zustand (act/stb) sich die Partner Plattform befindet.

Zur Realisierung muss dafür Sorge getragen werden, dass die kontrollierte Plattform selbständig aktiv wird, wenn für eine gewisse Zeit keine Kontrollkommandos vom Redundanz Partner gekommen sind. Ferner muss jede Quittung auf ein Kontrollkommando den Zustand (act/stb) des Empfängers des Kontrollkommandos enthalten. Darüber hinaus muss jede der beiden Plattformen bei jedem Zyklus (Kontrollkommando/ Quittung) den eigenen Zustand gegen den des Redundanz Partners (der Absender eines Kontrollkommandos muss immer aktiv sein) überprüfen. Liegt eine Inkonsistenz vor (z.B. beide Plattformen in aktivem Betriebszustand), kann dies z. B. dadurch behoben werden, dass dann jede der Plattformen in ihren Default Redundanz Zustand zurückfällt (der natürlich nur eine aktive Plattform

innerhalb des Redundanz Paares vorsieht). Zur Sicherheit sollte zusätzlich eine Prüfung des internen Kommunikationsnetzes stattfinden, um auszuschließen, dass ein Ausfall desselben dazu führt, dass mehrere Plattformen einer Redundanz-

5 einheit aktiv werden.

In Fig. 1 wird nun davon ausgegangen, dass eine der Redundanzeinheiten z. B. die Redundanzeinheit RU_t die kontrollierende Redundanzeinheit darstellt. Sie überwacht die Kommunikationsbeziehungen zwischen ihr selbst und allen Plattformen

10 $Plf_1 \dots Plf_k$ der kontrollierten Redundanzeinheit (z. B. RU_1). Die kontrollierende Redundanzeinheit RU_t setzt auch die Zustände (act/stb) auf allen Plattformen $Plf_1 \dots Plf_k$ der kontrollierten Redundanzeinheit RU_1 und ist dafür verantwortlich, dass diese konsistent sind, d.h. dass in der kontrollierten Redundanzeinheit RU_1 lediglich eine Plattform im aktiven Betriebszustand ist. Gleichzeitig wird die Redundanzeinheit RU_t von einer weiteren Redundanzeinheit kontrolliert. Dies kann beispielhaft die Redundanzeinheit RU_2 sein.

20 Fällt nun die Kommunikationsbeziehung zwischen der kontrollierenden Redundanzeinheit RU_t und der sich im aktiven Betriebszustand befindlichen Plattform der kontrollierten Redundanzeinheit RU_1 (z. B. Plattform k) für eine gewisse Zeit

25 aus, wird von der kontrollierenden Redundanzeinheit RU_t festgelegt, dass Plattform k ausgefallen ist (es könnte lediglich auch die Verbindung gestört sein, obwohl Plattform Plf_k in Ordnung ist). Als Konsequenz wird daraufhin eine andere Plattform der kontrollierten Redundanzeinheit RU_1 (z. B.

30 Plf_{k-1}) in den aktiven Betriebszustand und Plattform k (sobald diese wieder ansprechbar ist) in den bereitstehenden Betriebszustand geschaltet. Die Hochverfügbarkeit der kontrollierenden Redundanzeinheit RU_t erstreckt sich auch auf die Kontrollfunktion Control 1. Dies bedeutet, dass selbst bei

35 Teilausfall der kontrollierenden Redundanzeinheit RU_t die Funktion Control 1 noch zur Verfügung steht.

Mit der zweistufigen Kontrollfunktion lassen sich in einfacher Weise relevante Ausfallszenarien, Systemanlauf und Upgrade innerhalb der Redundanzsteuereinheit RCU beherrschen. Auch bei Ausfall mehrerer Plattformen kann jeweils immer die
5 theoretisch maximal mögliche Funktionalität zur Verfügung gestellt werden:

1. Ausfall einer aktiven Plattform:

10

Hier wird davon ausgegangen, dass die aktive, von der Plattform Plf3 kontrollierte Plattform Plf1 ausgefallen ist. Diese beantwortet somit die Kontrollkommandos der Plattform Plf3 nicht mehr. Die Plattform Plf3 überwacht, ob ihre Kontrollkommandos quittiert werden. Wenn für eine gewisse Anzahl Kontrollkommandos keine Quittung empfangen wurde und auch keine gegenteilige Indikation aus der Kommunikation mit der zu Plf1 redundanten Plattform Plf2 vorhanden ist, schließt die Plattform Plf3, dass Plf1 ausgefallen ist und setzt von nun an in
15 den Kontrollnachrichten an die Plattform Plf 1 den Parameter "go to stb" sowie in den Kontrollnachrichten an die Plattform Plf2 den Parameter "go to act". Die Plattform Plf2 geht daraufhin nach "act". Die Plattform Plf1 wird die Nachricht wegen Recovery oder Defekt in der Regel zunächst nicht empfangen. Irgendwann hat aber die Plattform Plf1 ihr Recovery beendet bzw. ist repariert und geht wieder in Betrieb, empfängt die Nachricht und geht nach "stb". Die Plattform Plf1 könnte zugleich aber die Kontrolle (Control 1) über das ihre Redundanzeinheit kontrollierende Redundanzpaar, also die
25 Plattformen Plf3 und Plf4, haben. Mit dem Ausfall der Plattform Plf1 fällt dann auch die Kontrollfunktion Control 1 aus, was im kontrollierten Redundanzpaar zunächst zu keinen Änderungen der "act/stb" Konfiguration führen sollte. Die Plattformen Plf3/ Plf4 arbeiten damit unverändert weiter. Nach relativ kurzer Zeit ist dann die Plattform Plf 2 in "act" und
30 übernimmt nach unserer Annahme "Control 1" über die Plattformen Plf3/4. Diese Übernahme führt ebenfalls in aller Regel

nicht zu einem Umschalten zwischen Plf3 und Plf4.

2. Ausfall einer Standby-Plattform:

5

Hier wird davon ausgegangen, dass die Plattform Plf2 ausgefallen ist. Der Ausfall führt nicht zu einem Umschalten durch die Plattform Plf3. Die Plattform Plf3 schickt weiterhin Kommandos mit "go to act" an die Plattform Plf1 und "go to stb" an die Plattform Plf2. Irgendwann hat die Plattform Plf2 ihr Recovery beendet bzw. ist nach Reparatur wieder verfügbar, empfängt das Kommando mit "go to stb" und geht entsprechend nach stb.

15

3. Doppelausfall eines Redundanzpaares:

Hier wird davon ausgegangen, dass die Plattformen Plf1 und Plf2 ausgefallen sind. Wenn die letzte Plattform Plf des Redundanzpaares ausgefallen ist, ist die act/stb Information des Kontrollierers (Plf3) ungültig und sollte gelöscht werden. Dementsprechend setzen Kontrollkommandos ab diesem Zeitpunkt den Parameter "go to act/stb" nicht mehr. Die Kontrollkommandos werden aber weiterhin an beide Plattformen geschickt. Die erste Plattform, die das Kommando quittiert, wird im Kontrollierer als "act" gekennzeichnet (die Quittung enthält ja den act/stb Zustand des Empfängers des Kontrollkommandos nicht). Ab diesem Zeitpunkt kann in den Kontrollkommandos wieder "go to act/stb" gesetzt sein. Damit ist sichergestellt dass, wann immer eine der beiden Plattformen eines Redundanzpaares verfügbar ist, diese sofort im Zustand "act" ist und die Services der Plattform bedient.

Mit dem Doppelausfall der Plattformen Plf1 und Plf2 fällt auch die Kontrollfunktion Control 1 von Plf1/Plf2 über Plf3/Plf4 aus. Dies wird in den Plattformen Plf3/Plf4 bemerkt. Nach einer gewissen Schutzzeit, die länger sein soll-

te, als das unter 1. beschriebene Umschalten dauert, wird die Auswertung der Kontrollfunktion Control 2 auf Plf3/Plf4 aktiviert, sofern nicht dauerhaft aktiv. Diese stellt,, wie oben beschrieben, immer noch eine Ersatzschaltfunktion auf
5 Plf3/Plf4 zur Verfügung. Dies bedeutet, dass die aus den Plattformen Plf3/Plf4 bestehende Redundanzeinheit unverändert ihre Services zur Verfügung stellt und immer noch hochverfügbar ist.

10 Fällt jetzt z.B. noch die Plattform Plf3 als aktive Plattform aus, so bemerkt Plattform Plf4, dass die Kontrollkommandos der Plattform Plf3 ausbleiben und geht nach einer gewissen Zeit selbst nach "act". Dies bedeutet, dass auch bei 3 ausgefallenen Plattformen innerhalb der Redundanzsteuereinheit die
15 vierte grundsätzlich "act" ist und den unter diesen Umständen maximalen Service zur Verfügung stellt. Sie bedient auch die Kontrollfunktion Control 1 gegenüber den Plattformen Plf1/Plf2 und auch die Kontrollfunktion Control 2 gegenüber der Plattform Plf3. D.h., wenn eine von diesen Plfs wieder
20 verfügbar wird, geht sie automatisch in den für sie richtigen Zustand.

Insbesondere im Falle, dass die Steuerung nur noch über die Kontrollfunktion 2 erfolgt, ergibt sich eine erhöhte Gefahr, dass die Situation eines Split Brain wegen gestörter Kommuni-
25 kation zwischen den Plattformen entsteht. Dieser Gefahr wird durch Verwendung eines mindestens gedoppelten Nachrichtenverteilsystems zwischen den beteiligten Plattformen entgegen gewirkt.

30

4. Systemanlauf:

Im Normalfall beendet eine beliebige Plattform im Quadrupel als erste ihr Recovery. Es kommt daher nicht zu Überschnei-
35 dungen von Kontrollnachrichten. Wenn eine Plattform das Recovery ihrer sonstigen Funktionalität (bis auf die Redundanzkontrolle) abgeschlossen hat und somit lauffähig ist, muss

sie für die Redundanzkontrolle ein spezifisches Handling durchlaufen, um zu entscheiden, ob sie sich im Sinne der Redundanzkontrolle im Zustand "act" oder "stb" befindet. Dazu definiert sie eine gewisse Schutzzeit, in der sie horcht,
5 welche Kontrollkommandos sie empfängt. Drei Fälle sind zu unterscheiden:

(i) Die Plattform empfängt ein Kommando nach "Control 1" (mit oder ohne zusätzlichen Empfang eines Kommandos nach "Control
10 2). Daraufhin wird für die Plattform "Control 1" aktiviert. Sie bekommt spätestens im nächsten "Control 1" Kommando mitgeteilt, ob sie "act" oder "stb" ist.

(ii) Die Plattform empfängt zwar kein Kommando nach „Control
15 1“, aber ein Kommando nach "Control 2". Hieraus zieht die Plattform den Schluss, dass ihr Redundanz Partner sich im Zustand "act" befindet und geht dementsprechend nach "stb".

(iii) Die Plattform empfängt weder ein Kommando nach „Control
20 1“ noch eines nach „Control 2“. Hieraus zieht die Plattform den Schluss, dass ihr Redundanz Partner sich nicht im hochgefahrenen Zustand befindet und geht selbst nach "act".

Der Normalfall ist, dass eine Plattform der beteiligten Redundanzeinheiten als erste ihr Recovery beendet. Beenden jedoch in einer Menge sich untereinander kontrollierender Redundanzeinheiten Plattformen ihr Recovery so kurz hintereinander, dass der Mechanismus der Kontrollfunktion Control 1 nicht für konsistente (act/stb) Zustände der jeweils kontrollierten Redundanzeinheit sorgen kann, werden alle diese
30 Plattformen damit praktisch gleichzeitig selbständig "act". Dies ist kein Problem, denn die jeweils kontrollierten "act" Plattformen übernehmen die Steuerfunktion Control 1 über die zu kontrollierenden Plattformen und „lernen“ im folgende deren Zustand (zumindest der "act" Plattform) . Dies bedeutet,
35 dass die Kontrollfunktion Control 1 sich der gegebenen Verteilung anpasst.

Das erfindungsgemäße Verfahren zeichnet sich insbesondere durch Abdeckung des folgenden Sonderfalls aus:

5 Beenden beide Plattformen in einem Redundanzpaar ohne Kontrolle gemäß Control 1 so kurz hintereinander ihr Recovery bzw. ihren Wiederanlauf nach Reparatur, dass der Mechanismus der Kontrollfunktion Control 2 nicht für einen konsistente (act/stb) Zustände sorgen kann, gehen zunächst beide Plattformen des Redundanzpaares selbständig nach "act" und senden
10 Kontrollkommandos an den Redundanzpartner. Dies wird aber von beiden Plattformen sofort bemerkt, und der oben beschriebene Korrekturmechanismus greift. Beide Plattformen gehen in ihren per Administration oder fester Programmierung definierten Default (act/stb) Zustand. Damit ist die Konsistenz wieder her-
15 gestellt.

5. System Upgrade:

Auch diese Aktion lässt sich mit dem vorgeschlagenen Verfahren
20 sehr leicht und unter der minimalen Einbusse der Systemstabilität der Redundanzeinheiten durchführen. Hierzu wird zunächst eine der Plattformen eines Redundanzpaares, z.B. die Plattform Plf1 außer Betrieb genommen. Daraufhin wird die Plattform Plf2 automatisch in den aktiven Betriebszustand gesteuert (wenn sie es nicht schon war), die
25 Kontrollfunktion Control 1 bleibt beiderseitig aktiv. Damit ist immer noch eine sehr hohe Verfügbarkeit und Sicherheit der 3 verbliebenen, funktionsfähigen Plattformen gegeben. Optional kann natürlich gezielt die "stb" Plattform außer Betrieb
30 genommen werden, so dass man an dieser Stelle überhaupt keine Beeinträchtigung der Services hat. Im Weiteren wird die außer Betrieb genommene Plattform Plf1 mit der neuen Software geladen und wieder hochgefahren. Der Plattform Plf1 wird ein Standby-Betriebszustand zugewiesen, die anderen Zustände im
35 Quadrupel ändern sich nicht.

Die aktive Plattform Plf2 im selben Redundanzpaar wird nun außer Betrieb genommen, wodurch automatisch die Plattform Plf1 in den aktiven Betriebszustand geht. Damit ist der SW Upgrade in Betrieb. Die Kontrollfunktion Control 1 ist nach
5 ganz kurzem Ausfall wieder beidseitig vorhanden. Nach Laden der neuen Software auf die Plattform Plf2, wird diese hochgefahren. Der Plattform Plf2 wird der Standby-Betriebszustand zugewiesen, die anderen Zustände im Quadrupel ändern sich nicht. Damit ist der SW Upgrade im Redundanzpaar (Plf1, Plf2)
10 komplett durchgeführt. Schließlich wird mit weiteren Redundanz Paaren (Plf3, Plf4) ebenso verfahren. Zur Verkürzung des für ein Upgrade notwendigen Zeitbedarfs kann alternativ auch die gleichzeitige Außerbetriebkonfiguration und Neuladen der STB Plattformen erfolgen, gefolgt von der Außerbetriebnahme
15 und dem Neuladen der bisherigen ACT Plattformen.

In Fig. 3 ist eine Konfiguration in einem Kommunikationssystem beschrieben, die die vorstehend beschriebene Architektur integriert. Dabei entsteht das Problem, dass externe Einrichtungen den Zustand der Plattformen und ggf. die Struktur der Redundanzeinheiten nicht kennen, obwohl sie die Plattformen ggf. überwachen. Ein Beispiel für derartige Einrichtungen sind Server Farm Architekturen eines Vermittlungssystems. Eine Server Farm besteht hierbei üblicherweise aus einem Server
20 Farm Controller und mehreren Servern. Der Server Farm Controller verteilt den hereinkommenden Verkehr nach gewissen Kriterien auf die Server, die aus seiner Sicht verfügbar sind. Um dies herauszufinden, überwacht er die Server mit Hilfe eines Kontrollprotokolls. Sind nun die Server identisch
25 mit den Plattformen der vorstehend beschriebenen Redundanzeinheiten, so berücksichtigt dieses Protokoll die oben angesprochenen "act/stb" Zustände innerhalb der Redundanzeinheit nicht. Diese Zustände lassen sich nicht ohne weiteres in einen existierenden Überwachungsmechanismus integrieren, da sie
30 ja nur applikationsspezifisch wirken. Dies bedeutet, dass für bestimmte Applikationen auch "stb" Plattformen voll funktionsfähig sein können. Für andere Applikationen dagegen muss

die Funktion völlig deaktiviert sein, weil der Redundanzpartner die alternativ aktivierbare Funktion bereitstellt. Da eine "stb" Plattform in der Regel aus Sicht des Betriebssystems und aller Applikationen, die nicht direkt mit dem beschriebenen Redundanzmechanismus in Verbindung stehen, aktiv ist, wird der Server Farm Controller Nachrichten auf sie verteilen. Dies gilt auch für Applikationen, die auf der Plattform deaktiviert sein müssen.

10 Hierbei können zwei Prinzipien zur Anwendung kommen: Gemäß dem ersten Prinzip nutzt der Server Farm Controller die Plattformen im Load Sharing Betrieb und gibt Aufträge an alle Plattformen einer Redundanzeinheit heraus, obwohl nach dem erfindungsgemäßen Redundanzmechanismus nur ein einziger davon in der Lage ist, diese Aufträge zu bedienen (Fig. 3). Hierzu wird eine sogenannte "Relay" Funktion eingeführt. Die Relay Funktion bewirkt, dass Nachrichten, die über eine interne Kommunikationsschnittstelle auf eine "stb" Plattform geschickt werden (1), von dieser unbesehen an ihren "act" Redundanz Partner weitergeschickt werden (2). Die aktive Plattform verarbeitet diese Nachrichten so, als wären sie direkt vom Server Farm Controller gekommen. Wenn eine Quittung zurückgeschickt werden muss, wird diese entweder von der aktiven Plattform direkt zum Server Farm Controller zurückgeschickt (5) oder sie geht den Weg zurück über die Standby-Plattform (5'), (6'). Die Relay-Funktion wird nur für die Applikationen aktiviert, für die das erfindungsgemäße Verfahren relevant ist und für die es folglich erforderlich ist, dass alle Nachrichten vom Server Farm Controller auf aktive Plattformen verteilt werden. Damit wird der gesamte Redundanzmechanismus (Redundanzkontrolle) vor dem Server Farm Controller verborgen. Deshalb entsteht dort kein Änderungsaufwand bei Einführung der Redundanz Kontrollfunktion auf den Plattformen der Server Farm.

35

Alternativ hierzu nutzt der Server Farm Controller die Redundanzeinheit insbesondere ein Redundanzpaar bereits nach einem

selbst definierten Active/Standby-Modus, der nur zufällig oder zumindest nicht sicher mit dem durch das erfindungsgemäße Verfahren bestimmten zusammenzufallen braucht. In letzterem Fall wird die alternative Nutzung durch die Ansprechbarkeit

5 des vom Server Farm Controller ausgewählten Redundanzpartners oder durch explizite, applikationsspezifische Kommunikation zwischen dem von dem Server Farm Controller ausgewählten Redundanzpartner und dem Server Farm Controller festgelegt. Hierzu deaktiviert die sich im Standby-Zustand befindliche

10 Plattform ihre Kommunikation zum Server Farm Controller, so dass dieser zwangsläufig auf die verbleibende aktivierte Plattform umschaltet. Alternativ hierzu informiert die Applikation auf der von dem Standby-Mode auf den Active-Mode geschalteten Plattformen den Server Farm Controller auf Appli-

15 kationslevel über die Verfügbarkeit der Plattform im Hinblick auf die Applikation. Hierzu kann ggf. eine bestehende oder eine neue Schnittstelle benutzt werden, wodurch eventuell geringer Anpassungsaufwand im Server Farm Controller entstehen kann.

Patentansprüche

1. Verfahren zur Redundanzkontrolle von elektrischen Einrichtungen (RU₁...RU_n),
5 dadurch gekennzeichnet,
dass die Redundanzkontrolle eine Funktionalität (Control 1) beinhaltet, mittels der jede der elektrischen Einrichtungen (RU₁...RU_n) von einer jeweils weiteren elektrischen Einrichtung überwacht wird,
10 dass die Redundanzkontrolle eine weitere Funktionalität (Control 2) beinhaltet, mittels der innerhalb der elektrischen Einrichtung (RU₁...RU_n) angeordnete internen Einrichtungen (Plf) sich gegenseitig überwachen,
dass die Funktionalität (Control 1) und die weitere Funktio-
15 nalität (Control 2) in jeder elektrischen Einrichtung eine in einem aktiven Betriebszustand befindliche interne Einrichtung und wenigstens eine hierzu redundante, in einem Standby-Betriebszustand befindliche interne Einrichtung definieren,
und die internen Einrichtungen (Plf) untereinander Steuer-
20 nachrichten über ein Nachrichtenverteilsystem austauschen.
2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
dass eine elektrische Einrichtung wenigstens eine weitere e-
25 lektrische Einrichtung überwacht.
3. Verfahren nach Anspruch 1, 2,
dadurch gekennzeichnet,
dass die weitere Funktionalität lediglich auf der überwachten
30 elektrischen Einrichtung aktiv ist.
4. Verfahren nach Anspruch 1 bis 3,
dadurch gekennzeichnet,
dass der aktive Betriebszustand sich über die alternative
35 Verfügbarkeit einer auf genau einer internen Einrichtung zu einem Zeitpunkt verfügbaren Ressource definiert.

5. Verfahren nach Anspruch 1 bis 4,
dadurch gekennzeichnet,
dass die Ressource die Kommunikationsfähigkeit über eine über
alle internen Einrichtungen der elektrischen Einrichtung ein-
heitliche IP Adresse darstellt.

6. Verfahren nach Anspruch 1 bis 5,
dadurch gekennzeichnet,
dass Kontrollnachrichten zwischen den internen Einrichtungen
vorgesehen werden, die von einer internen Einrichtung (Plf)
in der überwachenden elektrischen Einrichtung gesendet werden
und mit denen der empfangenden internen Einrichtung mitge-
teilt wird, dass sie in den aktiven oder Standby-Betriebs-
zustand gehen soll.

7. Verfahren nach einem der vorstehenden Ansprüche,
dadurch gekennzeichnet,
dass zwischen redundant angeordneten internen Einrichtungen
einer elektrischen Einrichtung ($RU_1 \dots RU_n$) eine Funkionali-
tät (RELAY) vorgesehen wird, mittels der die von einer über-
geordneten Einrichtung (SFC) erhaltenen Nachrichten, die auf
eine sich im Standby-Betriebszustand befindliche interne Ein-
richtung gesendet werden (1), von dieser über eine Kommunika-
tionsschnittstelle an ihren sich im aktiven Betriebszustand
befindlichen Redundanzpartner weitergeleitet werden (2).

8. Verfahren nach einem der Ansprüche 1 bis 4,
dadurch gekennzeichnet,
dass die sich im Standby-Betriebszustand befindliche interne
Einrichtung einer elektrischen Einrichtung ($RU_1 \dots RU_n$) ihre
Kommunikation zur übergeordneten Einrichtung (SFC) deakti-
viert, so dass diese zwangsläufig auf die verbleibende akti-
vierte Plattform umschaltet.

9. Vorrichtung zur Redundanzkontrolle von elektrischen Ein-
richtungen ($RU_1 \dots RU_n$),

- dadurch gekennzeichnet,
dass Mittel vorgesehen sind, mittels denen jede der elektrischen Einrichtungen ($RU_1 \dots RU_n$) von einer weiteren der elektrischen Einrichtungen überwacht wird, und zugleich ihrerseits
- 5 keine oder wenigstens eine der elektrischen Einrichtungen überwacht,
dass Mittel vorgesehen sind zur gegenseitigen Überwachung und Steuerung der internen Einrichtungen einer jeden elektrischen Einrichtung,
- 10 dass die Überwachung und Steuerung zu der Definition einer einzigen aktiven internen Einrichtung in jeder der elektrischen Einrichtungen führt,
dass die Mittel zur Überwachung und Steuerung die Kommunikationsfunktionen eines Nachrichtenverteilsystems nutzen.
- 15

FIG 1

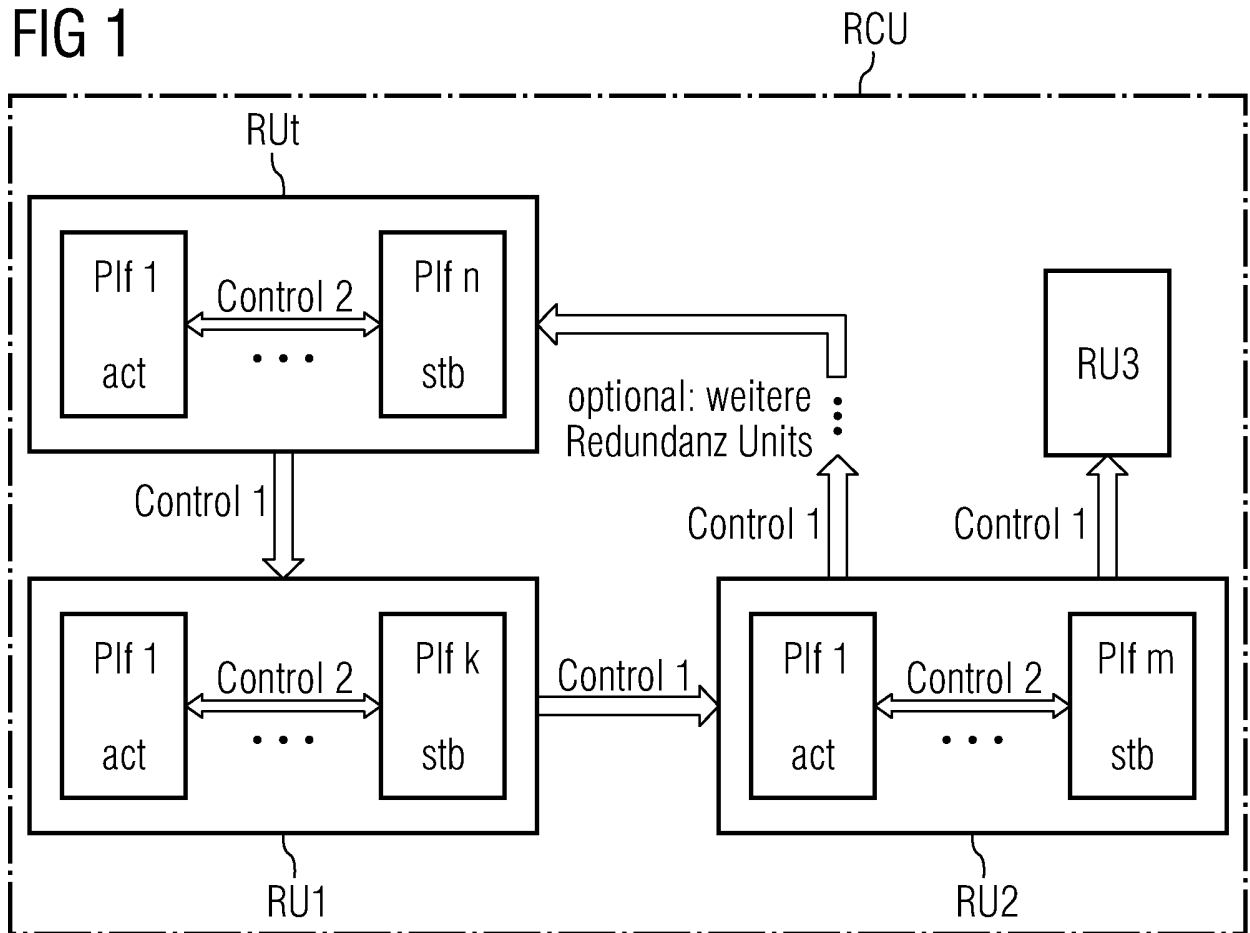


FIG 2

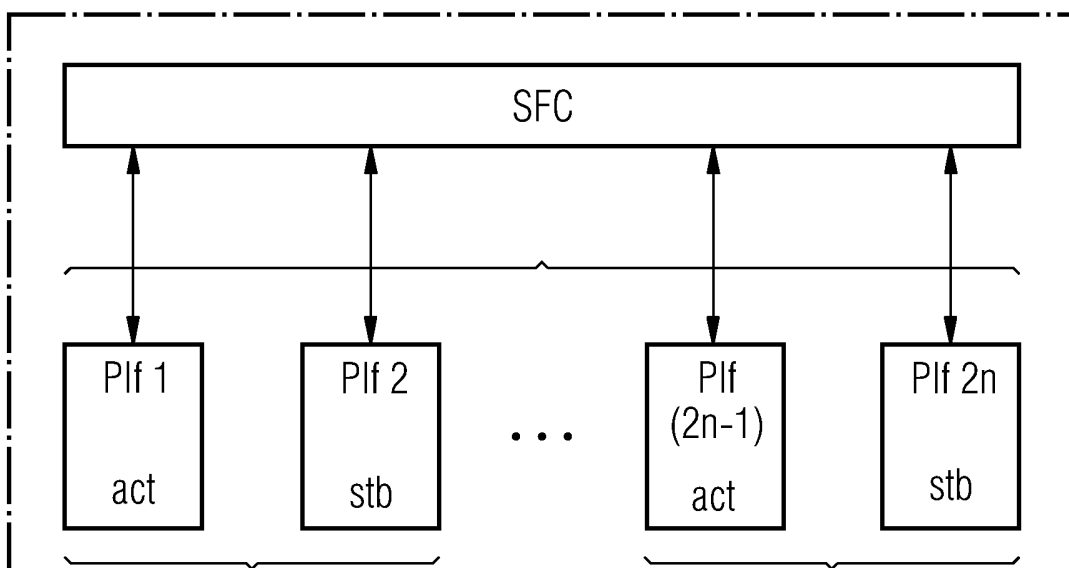


FIG 3

