(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 603 07 230 T2** 2007.07.05

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 471 673 B1**
(21) Deutsches Aktenzeichen: **603 07 230.5**
(96) Europäisches Aktenzeichen: **03 290 981.4**
(96) Europäischer Anmeldetag: **22.04.2003**
(97) Erstveröffentlichung durch das EPA: **27.10.2004**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **02.08.2006**
(47) Veröffentlichungstag im Patentblatt: **05.07.2007**

(51) Int Cl.[8]: ***H04J 3/08*** (2006.01)
H04L 12/437 (2006.01)

(73) Patentinhaber:
Alcatel Lucent, Paris, FR

(74) Vertreter:
Dreiss, Fuhlendorf, Steimle & Becker, 70188 Stuttgart

(84) Benannte Vertragsstaaten:
AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LI, LU, MC, NL, PT, RO, SE, SI, SK, TR

(72) Erfinder:
Mascolo, Vittorio, 26855 Lodivecchio (Lodi), IT

(54) Bezeichnung: **Verfahren zur Verwendung der gesamten Resourcenkapazität in einem SDH-Netzwerk mit einem Verkerrsschutzmechanismus, in Gegenwart von einem paketorientierten Datennetzwerk, und dazugehörender Apparat zur Durchführung des Verfahrens**

Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren für das Ausnutzen der vollen Ressourcenkapazität eines synchronen digitalen hierarchischen Netzwerks, das mit einem Schutzmechanismus ausgestattet ist, in Gegenwart eines Daten- (Packet) Netzwerks, und eine entsprechende Einrichtung zum Ausführen des Verfahrens.

[0002] Wenn ein Packet-Datennetzwerk auf einer synchronen hierarchischen Netzwerk- (wie SDH oder SONET) Infrastruktur aufgebaut wird, werden sowohl TDM- (Time Division Multiplex (= Zeitmultiplex)) als auch Daten- (Packet) Verkehr übertragen. Im Folgenden wird das synchrone digitale hierarchische Netzwerk mit dem Begriff SDH/SONET bezeichnet.

[0003] Bei einem SDH/SONET Netzwerk wird, wenn es in einer Ringkonfiguration organisiert ist, der wohlbekannte MS-SPRING Mechanismus als eines der verbreitetsten Schutzsysteme eingesetzt, wie im Standard ITU-T G.841 beschrieben, wobei die Transportkapazität zwischen Betriebs- und Schutz-Kapazität/Kanälen aufgeteilt ist. Jeder Betriebskanal hat einen entsprechenden Schutzkanal, der vom MS-SPRING Schutzmechanismus benutzt wird, um den Verkehr des Betriebskanals im Fehlerfall wieder herzustellen.

[0004] Unter normalen fehlerfreien Bedingungen übertragen die Betriebskanäle Daten- und TDM Verkehr, und die Schutzkanäle können benutzt werden, den so genannten "Extraverkehr" mit niedriger Priorität zu übertragen.

[0005] Im Fehlerfall jedoch wird der "Extraverkehr" in den Schutzkanälen vom MS-SPRING Mechanismus mit Beschlag belegt, um zu ermöglichen, dass der Verkehr der Betriebskanäle wieder hergestellt wird.

[0006] Deshalb hat dieser Schutzmechanismus den Hauptmangel, dass in der Praxis 50% der globalen SDH/SONET Kapazitätsressourcen verschwendet werden und gewöhnlich nicht für den Datentransport genutzt werden, nur deshalb, weil dieser Verkehr im Fehlerfalle mit Beschlag belegt werden müsste, wodurch die Zuverlässigkeit der Übertragung des Extraverkehrs drastisch reduziert würde.

[0007] Dieses Problem ist besonders wichtig wegen des großen Bedarfs an Datentransport über SDH/SONET, und deshalb muss die SDH/SONET Kapazität effizienter genutzt werden.

[0008] Die gleichen Überlegungen sind anwendbar bei der allgemeineren Situation von Ring- oder Maschennetzwerken, bei denen andere Schutzmassnahmen angewendet werden wie ein Ring SNCP (Sub-Network Connection Protection (= Unternetzwerkschutz)), wobei eine Schutzkapazität mit N Betriebskapazitäten geteilt wird.

[0009] Die Europäische Patentanmeldung EP 1 414 193, ein Mitglied der WO 03 015 351-Familie, beschreibt ein Kommunikationsverfahren für ein Netzwerk, das TDM Verkehr und Datenverkehr überträgt, wobei eine Vielzahl von Kommunikationseinrichtungen miteinander verbunden sind und eine Vielzahl von Paaren von Betriebskanälen und Backupkanälen auf zwei Pfaden zwischen benachbarten Kommunikationseinrichtungen eingesetzt werden, um 1:1 Schutzkommunikation durchzuführen.

[0010] Dieses Verfahren berücksichtigt nicht die Anwesenheit von möglichem Extraverkehr, der in den Kanälen niedriger Priorität konfigurierbar ist.

[0011] Deshalb ist die Hauptaufgabe der vorliegenden Erfindung, ein Verfahren anzugeben für das Ausnutzen der vollen Ressourcenkapazität eines SDH/SONET Netzwerks, das mit einem Schutzmechanismus ausgestattet ist, in Gegenwart eines Daten- (Packet) Netzwerks.

[0012] Es ist eine weitere Aufgabe, eine Einrichtung für die Ausführung der Erfindung bereitzustellen.

[0013] Die Grundidee der vorliegenden Erfindung ist, die komplette SDH/SONET Schutz (Reserve) Kapazität unter normalen und unter Fehlerbedingungen für die Übertragung von Datenverkehr zu nutzen.

[0014] Detaillierter betrachtet überträgt die Betriebskapazität im fehlerfreien Betrieb TDM und jeden Typ von Datenverkehr (mit hoher, mittlerer und niedriger Priorität), während die Schutzkapazität nur Datenverkehr niedriger Priorität transportieren kann.

[0015] Im Fehlerfall wird die Betriebskapazität unterbrochen, und

- der TDM Verkehr wird zum Gegenstand des bekannten Schutzmechanismus und wird übergeleitet auf die Schutzkapazität, wobei
- ein Teil des Extra Datenverkehrs mit hoher (und mittlerer) Priorität übergeleitet wird auf die Schutzkapazität, und
- ein Teil des Datenverkehrs mit niedriger Priorität (der bei normalen Bedingungen über die Schutzkapazität übertragen wird) die verbleibende Schutzkapazität mit dem Best Effort-Teil des Datenverkehrs mit niedriger Priorität teilt, der bei normalen Bedingungen über die Betriebskapazität übertragen wird.

[0016] Bei einem abgeänderten Ausführungsbeispiel überträgt die Schutzkapazität auch den weiter unten definierten NUT Verkehr (Not pre-emptable Unprotected Traffic (= nicht mit Beschlag belegbarer

ungeschützter Verkehr)), sowohl bei normalen als auch unter Fehlerbedingungen.

[0017] Das Verfahren, das Gegenstand der Erfindung ist, ist anwendbar bei jeder Art von SDH/SONET Netzwerken, Ring- oder Maschennetzen, physikalischen und virtuellen, und bei Anwendung von jedem bekannten Schutzmechanismus, wie MS-SPRING, SNCP oder anderen.

[0018] Diese und weitere Aufgaben werden gelöst durch ein Verfahren und eine Einrichtung, wie in den anhängenden Ansprüchen beschrieben, die als integraler Bestandteil der vorliegenden Beschreibung angesehen werden.

[0019] Die Erfindung wird erklärt mit Hilfe der folgenden detaillierten Beschreibung, die als lediglich beispielhaftes und nicht als beschränkendes Exempel gegeben wird, und mit Bezug auf die anhängenden Zeichnungen zu lesen ist, in denen:

[0020] Fig. 1 eine schematische Darstellung eines bekannten SDH/SONET Knotens eines ringähnlichen Netzwerks ist;

[0021] Fig. 2 das Verhalten des SDH/SONET Knotens im Fehlerfall entsprechend einer ersten Variante der Erfindung zeigt;

[0022] Fig. 3 und Fig. 4 das Verhalten des SDH/SONET Knotens entsprechend einer zweiten Variante der Erfindung zeigt bei Anwesenheit einer NUT Datenverkehrkomponente;

[0023] Fig. 5, Fig. 6 und Fig. 7 den inneren Aufbau eines SDH/SONET Knotens für die Ausführung der Erfindung zeigt.

[0024] Mit Bezug auf Fig. 1 zeigt NE eine schematische Darstellung eines bekannten SDH/SONET Knotens eines ringähnlichen Netzwerks, in dem der bekannte MS-SPRING Schutzmechanismus angewendet wird. Der Ring kann ein physikalischer oder ein virtueller Ring sein, das wäre ein Unternetzwerk, aufgebaut auf einer physikalisch vermaschten Topologie.

[0025] Zwischen den Knoten werden die Verbindungsressourcen durch die Betriebsverbindungskapazität WRK und die Schutz- (Reserve) Verbindungskapazität PROT bereitgestellt, wobei die Schutzverbindungskapazität normalerweise gleich der Betriebsverbindungskapazität ist.

[0026] Wenn ein Datenpacket-Netzwerk PKT über einer SDH/SONET Ring-Infrastruktur aufgebaut wird, müssen sowohl TDM- (Zeitmultiplex) als auch Daten-Verkehr (DATA) über den SDH/SONET Ring übertragen werden. Der Datenverkehr kann verschiedene Serviceklassen CoS (= Class Of Service) haben, abhängig vom Prioritäts-/Wichtigkeitsgrad.

[0027] Im Folgenden wird Bezug genommen auf die drei bekannten Serviceklassen: Serviceklasse hoher Priorität, Serviceklasse mittlerer Priorität, Serviceklasse niedriger (Best Effort) Priorität, selbst wenn klar ist, dass eine unterschiedliche Unterteilung anwendbar sein kann.

[0028] Der Datenverkehr mit hoher Priorität ist ein Datenverkehr mit garantierter Bandbreite und vollem anzuwendenden Schutzumfang, wie der TDM Verkehr; die CoS mit mittlerer Priorität ist ein Datenverkehr mit zwei Verkehrskomponenten, der einen mit garantierter Bandbreite, wie bei der hohen, und der anderen mit nicht garantierter Bandbreite; die CoS mit niedriger Priorität ist ein Best Effort Datenverkehr mit nicht garantierter Bandbreite.

[0029] Im Folgenden wird Datenverkehr mit DT-H bezeichnet, das ist der mit CoS hoher Priorität und der erste Teil der CoS mittlerer Priorität mit garantierter Bandbreite und vollem Schutz und mit DT-L bezeichnet, das ist der zweite Teil der CoS mittlerer Priorität mit nicht garantierter Bandbreite.

[0030] Im normalen fehlerfreien Betrieb überträgt die Betriebskapazität WRK den gesamten TDM Verkehr und den Datenverkehr DT-H und möglicherweise einen Teil des Datenverkehrs DT-L, abhängig von der Gesamtkapazität, während die Schutz (Reserve) Kapazität PROT benutzt sein kann oder nicht benutzt sein kann für die Übertragung von Extra Datenverkehr DT-L (im Folgenden mit Extra Traffic DT-L bezeichnet), abhängig von dem zuvor beschriebenen Beschlagnahmeproblem.

[0031] Mit Bezug auf Fig. 2 wird ein erstes Ausführungsbeispiel der Erfindung beschrieben, das den Fall der Reservekapazität PROT betrifft, die benutzt wird, um Datenverkehr der Best Effort Klasse zu übertragen. Im Falle eines Fehlers wird die Betriebskapazität WRK unterbrochen, und:
der TDM Verkehr ist Gegenstand des bekannten MS-SPRING Schutzmechanismus, wobei dieser als solcher zur Schutzkapazität PROT verschoben wird;
der Datenverkehr DT-H wird, wie der TDM Verkehr, zur Schutzkapazität PROT verschoben;
ein Teil des Extra-Traffics DT-L, der über die Reservekapazität PROT übertragen wurde, teilt die verbleibende Schutzkapazität PROT mit dem Datenverkehr DT-L, der über die Betriebskapazität WRK (und jetzt geschützt ist) übertragen wurde, entsprechend einem unten beschriebenen Verteilungsschema. Auf diese Weise wird der Best Effort Verkehr nicht mit Beschlag belegt, so gibt es keine Dienstunterbrechung, nur eine Dienstbeeinträchtigung wegen der gemeinsamen Nutzung der verfügbaren Transportressourcen des verbleibenden Teils DT-L1 der Schutzkapa-

zität PROT.

[0032] Mit Bezug auf Fig. 3 wird ein zweites Ausführungsbeispiel der Erfindung beschrieben, das den Fall betrifft, bei dem ein Teil der Schutzkapazität PROT reserviert ist, um den so genannten NUT (Not pre-emptive Unprotected Traffic (= nicht mit Beschlag belegbarer ungeschützter Verkehr) Datenverkehr zu übertragen, der von dem MS-SPRING Mechanismus weder benutzt noch mit Beschlag belegt werden kann. Die NUT Kapazität wird nur vom Datennetzwerk benutzt und bei Bedarf Gegenstand eines Schutzmechanismus auf der Schicht der Ebene L2 (d.h. RPR, ATM, ...).

[0033] Mit Bezug auf Fig. 4 wird im Fehlerfall die Betriebskapazität WRK unterbrochen und die Schutzkapazität PROT wird benutzt, wie im Ausführungsbeispiel von Fig. 1, aber der NUT Teil steht nicht zur Verfügung und muss so bleiben, wie er ist.

[0034] Als nicht beschränkendes Beispiel sei folgendes Szenario angenommen: Es müssen 10% TDM Verkehr und 80% Datenverkehr bei Verwendung einer typischen 2F MS-SPRING geschützten SDH/SONET Ring-Infrastruktur (X Kapazität mit X = 155, 622, 2400, 10 000 Mbps) übertragen werden. Bei der traditionellen bekannten Lösung werden 50% von X als Reservekapazität benutzt und stehen nicht zur Verfügung. Entsprechend diesem Vorschlag werden nur 10% dieser Kapazität als Reservekapazität verwendet (um den TDM Verkehr zu schützen, der 10% des gesamten Verkehrs umfasst). Die verbleibende Kapazität wird von den verschiedenen Typen von Datenverkehr gemeinsam genutzt.

[0035] Mit Bezug auf die Fig. 5, Fig. 6 und Fig. 7 wird im Folgenden beschrieben, wie das Netzwerkelement NE arbeitet, um das erfindungsgemäße Verfahren auszuführen.

[0036] Das Untersystem eines Netzwerkelements, das den MS-SPRING Schutzmechanismus verwaltet, kann dargestellt werden wie in Fig. 5 gezeigt: Es umfasst grundsätzlich ein APS Controller-Modul APS-CONTR und ein Aktuatormodul ACTUATOR.

[0037] Das APS-CONTR Modul verwaltet das Signalprotokoll, das von dem MS-SPRING Schutzmechanismus benutzt wird durch Betreiben der bekannten APS Maschine bei jedem Netzwerkelement NE des Netzwerks entsprechend dem SDH/SONET bidirektionalen Ringprotokoll (Standard ITU-T G.841).

[0038] Das APS-CONTR Modul ist grundsätzlich eine Statusmaschine, die die APS Maschine betreibt, die die Eingangsdaten analysiert, die kommen von:
eingehenden Signalprotokollen von APS Bytes des MS Overheads des SDH/SONET Rahmens;
extern ausgelöste Befehle;
erkannten Fehlern auf Betriebs- und/oder Schutzkanälen.

[0039] Das APS-CONTR Modul muss entsprechend den ITU-T G.841 Regeln das ausgehende Signalprotokoll für die APS Bytes des MS Overheads der ausgehenden SDH/SONET Rahmen abwickeln, und die weiteren "lokalen Aktionen", die vom Aktuatormodul über die Verbindungsmatrix des Cross Connects im Netzwerkelement durchzuführen sind, es muss nämlich die neuen Matrixverbindungen (für das Netzwerkelement) aufbauen, um die ausgefallene Betriebsvernetzung entsprechend den MS-SPRING Protokollregeln wieder herzustellen.

[0040] Das Verhalten des APS-CONTR Untersystems ist deshalb dergestalt, dass
der Fehlerdetektor die Auslöseereignisse für die APS Statusmaschine signalisiert;
die APS Statusmaschine das Signal-Schutzprotokoll entsprechend dem Ringstatus und den Auslöseereignissen betreibt;
die APS Statusmaschine entsprechend dem neuen Ringstatus, den Verkehrsübersichten und der Ringtopologie agiert, um die Betriebsverbindungen zu reparieren durch Manipulationen an den Cross Verbindungen durch den Aktuator.

[0041] Wie im Folgenden beschrieben, ist das APS-CONTR Modul des MS-SPRING Mechanismus von der vorliegenden Erfindung nicht betroffen, es verhält sich auf die bekannte Weise. Nur das Aktuatormodul ist betroffen.

[0042] Die Fig. 6 und Fig. 7 zeigen den inneren Aufbau des Switching-Teils TDM-SWC des Netzwerkelements NE und, wie es entsprechend der Erfindung, unter fehlerfreien und Fehlerbedingungen arbeitet.

[0043] TDM-SWC umfasst einen Switching Abschnitt für den TDM Verkehr, der von den Eingangsschnittstellen TDM-IF kommt und zu den Ausgangsschnittstellen TDM-OF geleitet wird, wobei im fehlerfreien Betrieb TDM Verkehr über den TDM Teil des Betriebskanals WRK gesendet wird.

[0044] Der durchgeleitete Verkehr wird zur Vereinfachung nicht dargestellt, weil der beschrieben wurde im Zusammenhang mit dem Verhalten eines Knotens, der den Verkehr erzeugt.

[0045] TDM-SWC umfasst weiterhin ein Switching Untersystem PKT-SWC für den Datenverkehr, der von den Eingangsschnittstellen PKT-IF kommt.

[0046] PKT-SWC umfasst:
ein Eingangs-Mappermodul MPR, das die Dienstklasse des Eingangsdatenverkehrs erkennt, Verkehr mit hoher (und mittlerer) Priorität DT-H oder mit niedriger Priorität DT-L. Der Anteil des Datenverkehrs mit

hoher Priorität wird unter fehlerfreien Bedingungen über den DATA Teil der Betriebskapazität WRK übertragen, weil er geschützt werden muss. Der Anteil mit niedriger Priorität kann entweder über den DATA Teil der Betriebskapazität WRK oder die Reservekapazität PROT übertragen werden, weil es sich um Best Effort Verkehr handelt und nicht geschützt werden muss;
ein Lastausgleichsmodul L-BAL, das die Aufgabe hat, den Datenverkehr den korrekten Ausgangsschnittstellen TDM-OF zuzuordnen, sowohl im fehlerfreien Betrieb als auch unter Fehlerbedingungen.

[0047] In der Praxis ist es die Aufgabe des Lastausgleichers L-BAL:
Abtrennen der Daten hoher Priorität von denen mit niedriger Priorität durch deren Einkartieren in verschiedene VCs (virtuelle Container) der SDH/SONET Rahmen, die einen gehören zur Betriebskapazität, die anderen zur Reservekapazität;
Anwenden einer Funktion von statistischem Multiplexen für den Datenverkehr niedriger Priorität für den Zugriff auf zugeordnete VCs; diese Funktion kann als statistisches Zeitmultiplexen (STDM (von Statistical Time Division Multiplex)) bezeichnet werden: es ist eine Form von Zeitmultiplex, wobei einem gegebenen Datenstrom dynamisch mehr oder weniger Bandbreite zugeteilt werden kann, basierend auf seinem Bedarf und dem Bedarf anderer Datenströme; dies ist bekannt und wird in Einrichtungen wie Routern, LAN Switches und Rahmenrelay Switches angewandt;
Ausgleichen des Datenverkehrs mit niedriger Priorität sowohl im fehlerfreien Betrieb als auch unter Fehlerbedingungen.

[0048] In dem bekannten System wird im Fehlerfall und nachfolgendem Schutzschaltvorgang der Betriebsverkehr auf die Schutzkanäle zugreifen, was Extra Verkehr erzeugt, der von den Schutzkanälen entfernt werden muss.

[0049] Mehr ins Detail gehend müssen bei dem bekannten MS-SPRING System die Knoten, die dem Fehler benachbart sind, eine so genannte "Bridge und Switch" Aktion managen. Alle anderen Knoten (Zwischenknoten) sind bei dem Schutzprozess nicht beteiligt; sie belegen nur ihren Extra Verkehr mit Beschlag, wodurch die Durchleitungsverbindungen über den Schutzkanal aufgebaut werden. Durch konsequente Anwendung beim Schutz-Switching (sowohl beim Strecken- als auch beim Ringtyp) werden alle Schutzkanäle benutzt, um den Betriebskanal zu ersetzen.

[0050] Bei der Erfindung dahingegen müssen nur der TDM Verkehr und der Anteil des Datenverkehrs mit hoher Priorität geschützt werden; ihr gesamter Anteil muss kleiner sein als die gesamte Betriebskapazität.

[0051] Mit Bezug auf Fig. 7 wird im Fehlerfall der TDM und der DT-H Verkehr umgeroutet auf die Reservekapazität PROT und der verbleibende Teil von PROT wird benutzt, um den DT-L Verkehr zu übertragen. Natürlich wird die Komponente niedriger Priorität DT-L entsprechend verwaltet, um zu garantieren, dass die Reserveressourcen dem geschützten verkehr (sowohl TDM als auch DT-H) zur Verfügung stehen, durch Anwenden der oben beschriebenen Funktion des statistischen Multiplexens.

[0052] Um dieses Merkmal zu ermöglichen, wird die Aktuatormaschine des MS-SPRING eingesetzt.

[0053] In dem bekannten MS-SPRING System führt die Aktuatormaschine im Fehlerfall nach dem Empfang des Startbefehls von der APS Maschine folgende Aktionen an allen Reservekapazitätsverbindungen aus:
den gesamten Verkehr niedriger Priorität stummschalten (AIS erzwingen, um Fehlverbindung zu vermeiden);
Bridge und Switch – veranlasst, dass die Cross-Connect-Fähigkeit den Betriebsverkehr wieder herstellt – es werden die gesamten Reservekapazitäts Ressourcen eingesetzt, um die Betriebsressourcen zu ersetzen;
AIS entfernen.

[0054] Erfindungsgemäß führt die Aktuatormaschine ACTUATOR von Fig. 5, auch in Fig. 6 und Fig. 7 gezeigt, im Fehlerfall folgende Aktionen an den Reservekapazitätsverbindungen aus:
teilweises Stummschalten des Verkehrs niedriger Priorität (AIS nicht auf der ganzen Kapazität erzwingen), nur den Teil mit Beschlag belegen, der für den Schutz des TDM- und des DT-H-Verkehrs benötigt wird;
Bridge und Switch – veranlasst, dass die Cross-Connect-Fähigkeit den Betriebsverkehr (TDM und DT-H) wieder herstellt – es werden nicht die gesamten Reservekapazitätsressourcen eingesetzt, um die Betriebsressourcen zu ersetzen;
AIS entfernen;
Ausgleichen des Zugangs für den Datenverkehr mit niedriger Priorität zu der verbleibenden Reservekapazität durch statistisches Multiplexen.

[0055] Im Fall der Anwesenheit einer NUT Verkehrskomponente verwaltet der Block PKT-SWC die NUT auf bekannte Weise, um sie in der PROT Kapazität unterzubringen.

[0056] Der Lastausgleicher L-BAL und der Aktuator sorgen dafür, dass die verschiedenen Verkehrskomponenten in der PROT Kapazität untergebracht werden, wobei die NUT Komponente sowohl unter normalen als auch unter Fehlerbedingungen unangetastet bleibt.

[0057] Weitere Implementierungsdetails werden nicht beschrieben, denn der Fachmann auf diesem Gebiet ist in der Lage, die Erfindung auszuführen, ausgehend von der Lehre der vorstehenden Beschreibung.

[0058] Beispielsweise ist die gleiche Technik anwendbar bei der allgemeineren Situation eines Ring- oder Maschennetzwerks, bei dem ein anderer Typ von Schutzmechanismus, wie SNCP (Sub-Network Connection Protection (= Unternetzwerkschutz)), wobei eine Schutzkapazität mit N Betriebskapazitäten geteilt wird. Auch im Fall des bekannten N:1 Schutzmechanismus, verhält sich die erste Betriebskapazität, die als Folge eines Fehlers auf die entsprechende Schutzkapazität verschoben wird, genau so wie im Fall des zuvor beschriebenen Beispiels der bekannten Systeme, und kann deshalb Gegenstand der Ausnutzung der gesamten Schutzressourcenkapazität des Verfahrens sein, das Aufgabe der Erfindung ist.

Patentansprüche

1. Verfahren für das Ausnutzen der vollen Ressourcenkapazität eines synchronen digitalen hierarchischen Netzwerks, das mit einem Schutzmechanismus ausgestattet ist, in Gegenwart eines Datennetzwerks, wobei besagtes Netzwerk Knoten umfasst, die bidirektional TDM-Verkehr (TDM), Datenverkehr mit hoher Priorität (DT-H) und Datenverkehr mit niedriger Priorität (DT-L) über Betriebs- (WRK) und Schutz- (PROT) Kapazität/Kanäle übertragen, und wobei das Verfahren folgende Schritte umfasst, falls bei einem der beteiligten Knoten ein Fehler auftritt:
– die Betriebskapazität wird unterbrochen; der TDM verkehr wird zum Gegenstand des besagten Schutzmechanismus und wird übergeleitet auf die Schutzkapazität;
dadurch gekennzeichnet, dass
– ein Teil des Datenverkehrs mit hoher Priorität (DT-H) übergeleitet wird auf die Schutzkapazität;
– veranlasst wird, dass ein Teil des Datenverkehrs mit niedriger Priorität (DT-L), der bei normalen Bedingungen über die Schutzkapazität übertragen wird, die verbleibende Schutzkapazität mit dem Teil des Datenverkehrs mit niedriger Priorität teilt, der bei normalen Bedingungen über die Betriebskapazität übertragen wird, auf eine Weise, dass die komplette Schutzkapazität benutzt wird, Datenverkehr sowohl bei normalen als auch bei Fehlerbedingungen zu übertragen.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass es den weiteren Schritt des Reservierens eines Teils der Schutzkapazität umfasst für das Übertragen von NUT (Not pre-emptive Unprotected Traffic (= nicht vorbeugend, ungeschützter Verkehr) Datenverkehr sowohl bei normalen als auch bei Fehlerbedingungen.

3. Verfahren nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, dass das besagte Teilen der verbleibenden Schutzkapazität zum Übertragen des Datenverkehrs mit niedriger Priorität durchgeführt wird durch Anwenden einer Funktion von statistischem Multiplexen des besagten Datenverkehrs mit niedriger Priorität, der sowohl von der Betriebskapazität als auch von der Schutzkapazität kommt, so dass es im Fehlerfall keine Dienstunterbrechung gibt, sondern lediglich eine Dienstbeeinträchtigung.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass in den besagten Netzwerkknoten eine Aktuatorfunktion an der Verbindungsmatrix des Cross-Connects durchgeführt wird, wodurch im Fehlerfalle neue Matrixverbindungen zu der Schutzkapazität aufgebaut werden, um die ausgefallene Betriebskapazität zu ersetzen, wobei die besagte Aktuatorfunktion verursacht, dass im Fehlerfall folgende Aktionen an der besagten Schutzkapazität durchgeführt werden:
– teilweises Unterdrücken des Datenverkehrs mit niedriger Priorität, der vor dem Fehler vorhanden war und vorbeugendes Schützen nur des Anteils, der zum Übertragen des besagten TDM-Verkehrs und des Datenverkehrs mit hoher Priorität erforderlich ist,
– Bridge und Switch: Betreiben der Cross-Connection-Matrix, um den TDM-Verkehr und den Datenverkehr mit hoher Priorität wieder herzustellen,
– Ausbalancieren des Zugangs für Datenverkehr mit niedriger Priorität auf die verbleibende Restkapazität durch das besagte statistische Multiplexen.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass das besagte Netzwerk ein Ringnetzwerk ist, das mit einem MS/SPRING Schutzmechanismus ausgestattet ist.

6. Netzwerkknoten zum Ausführen des Verfahrens nach einem der Ansprüche 3 bis 5, dadurch gekennzeichnet, dass er umfasst:
– ein erstes Switching Element (TDM-SWC) zum Switchen des TDM-Verkehrs über den TDM-Teil der Betriebskanäle (WRK) im fehlerfreien Betrieb und über die Schutzkapazität (PROT) im Fehlerfall;
– ein zweites Switching Element (PKT-SWC) für den Datenverkehr, bestehend aus Schaltungen, um folgende Aktionen durchzuführen:
– Erkennen der Dienstklasse der Eingangsdaten, den besagten Datenverkehr mit hoher (DT-H) oder niedriger (DT-L) Priorität;
– Zuordnen des Datenverkehrs zum korrekten Ausgang der besagten Betriebs- oder Schutzkapazität, sowohl beim fehlerfreien Betrieb als auch im Fehlerfall, so dass bei Fehlerbedingungen der gesamte Datenverkehr mit hoher Priorität (DT-H) auf die Schutzkapazität umgeswitched wird und der Datenverkehr mit niedriger Priorität (DT-L) entsprechend der be-

sagten Funktion des statistischen Multiplexens auf die Schutzkapazität umgeschaltet wird.

7. Netzwerkknoten nach Anspruch 6, dadurch gekennzeichnet, dass das besagte zweite Switching Element (PKT-SWC) umfasst:
– ein Eingangsmapper-Modul (MPR) für das besagte Erkennen der Dienstklasse der Eingangsdaten;
– ein Lastbalancier-Modul (L-BAL) für das besagte Zuordnen des Datenverkehrs zum korrekten Ausgang, sowohl beim fehlerfreien Betrieb als auch im Fehlerfall, wobei das besagte Lastbalanciermodul (L-BAL) Schaltungen umfasst zum
– Abtrennen der Daten mit hoher Priorität von denen mit niedriger Priorität durch Kartieren in verschiedene virtuelle Container (VCs) der synchronen digitalen Hierarchierahmen;
– Anwenden der besagten Funktion des statistischen Multiplexens für den Datenverkehr mit niedriger Priorität, um auf die zugeordneten VCs zuzugreifen;
– Ausgleichen des Datenverkehrs mit niedriger Priorität (DT-L) sowohl beim fehlerfreien Betrieb als auch im Fehlerfall, so dass der besagte Datenverkehr mit niedriger Priorität bei Fehlerbedingungen entsprechend der besagten Funktion des statistischen Multiplexens auf die Schutzkapazität umgeswitched wird.

8. Synchrones digitales hierarchisches Netzwerk, das mit einem Schutzmechanismus ausgestattet ist und einem darüber liegenden Datennetzwerk, wobei das besagte Netzwerk Mittel umfasst zum Ausführen des Verfahrens nach einem der Ansprüche 1 bis 5.

9. Synchrones digitales hierarchisches Netzwerk, das mit einem Schutzmechanismus ausgestattet ist und einem darüber liegenden Datennetzwerk, wobei das besagte Netzwerk Netzwerkknoten umfasst nach einem der Ansprüche 6 oder 7.

Es folgen 4 Blatt Zeichnungen

Anhängende Zeichnungen

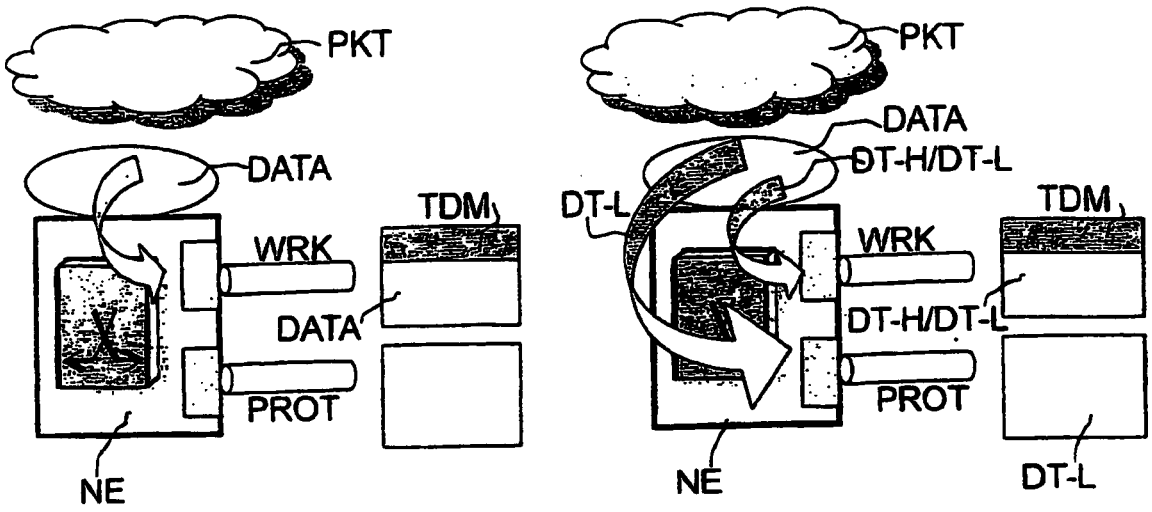

FIG. 1

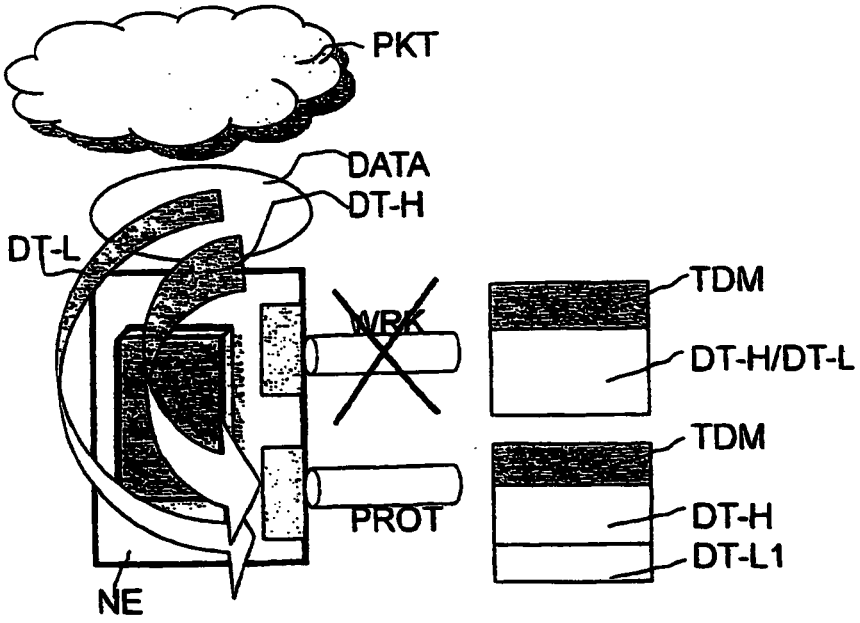

FIG. 2

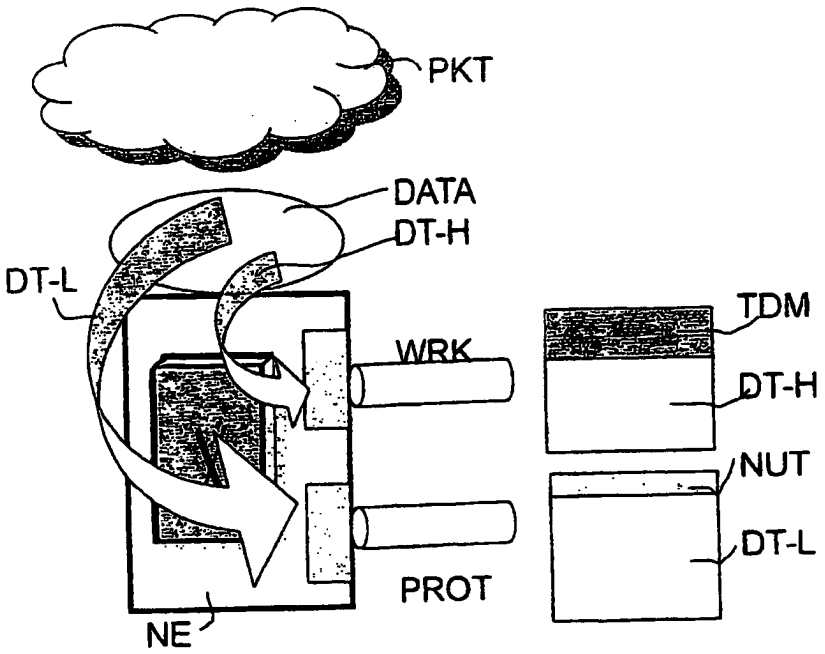
PKT
DATA
DT-H
DT-L
WRK
PROT
NE
TDM
DT-H
NUT
DT-L

FIG. 3

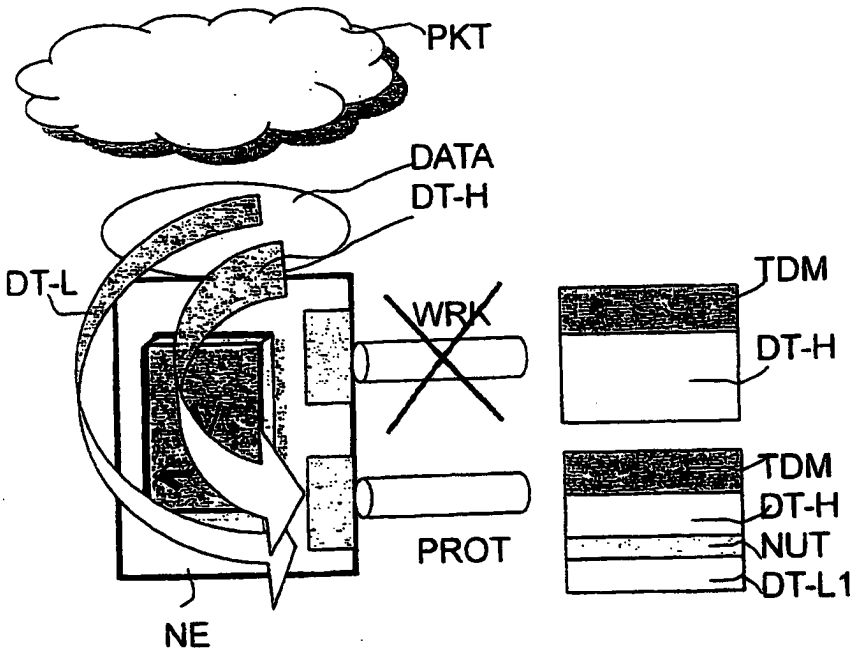
PKT
DATA
DT-H
DT-L
WRK
PROT
NE
TDM
DT-H
TDM
DT-H
NUT
DT-L1

FIG. 4

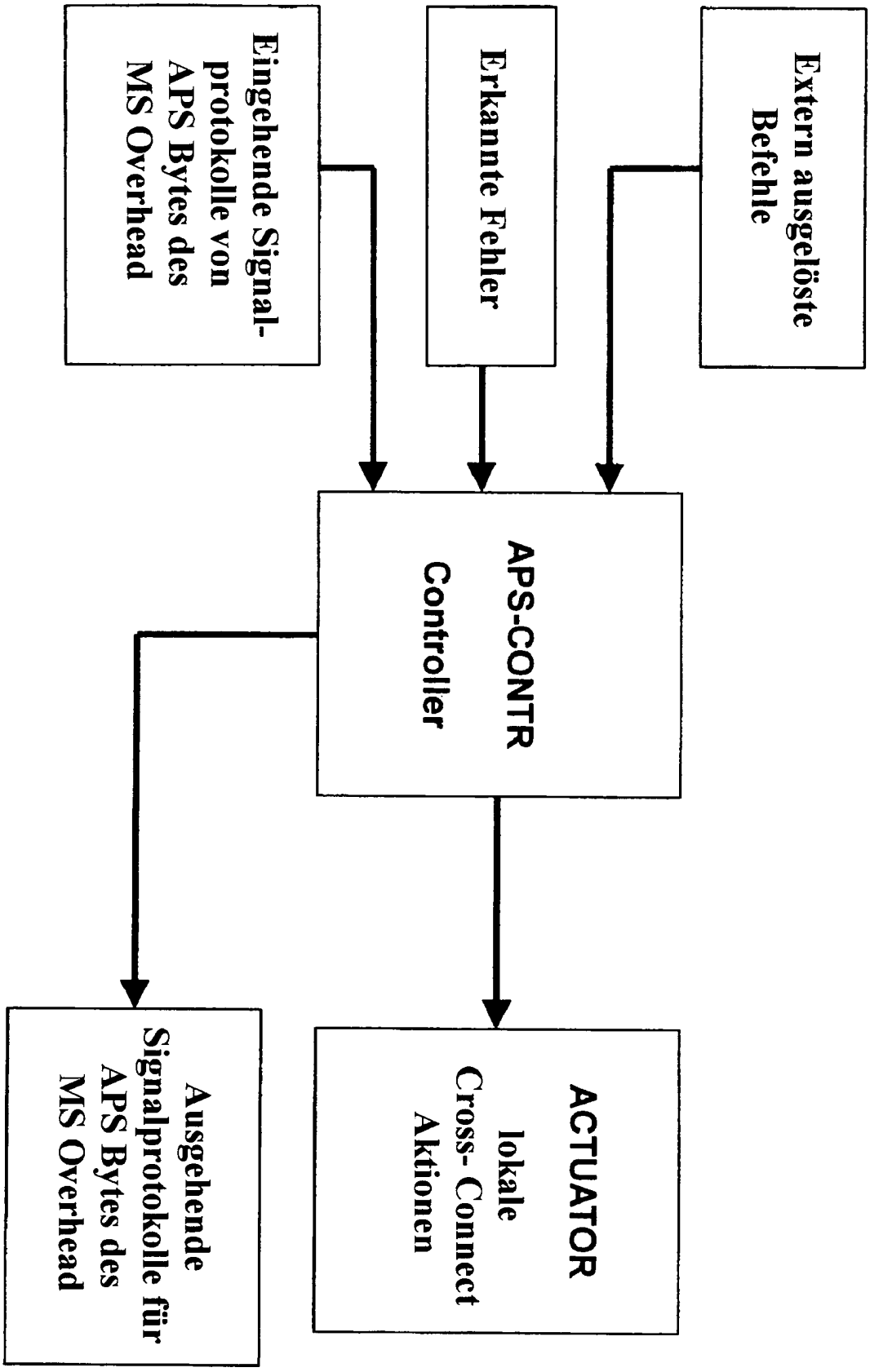
Extern ausgelöste Befehle
Erkannte Fehler
Eingehende Signal-protokolle von APS Bytes des MS Overhead
APS-CONTR Controller
ACTUATOR lokale Cross- Connect Aktionen
Ausgehende Signalprotokolle für APS Bytes des MS Overhead

FIG. 5

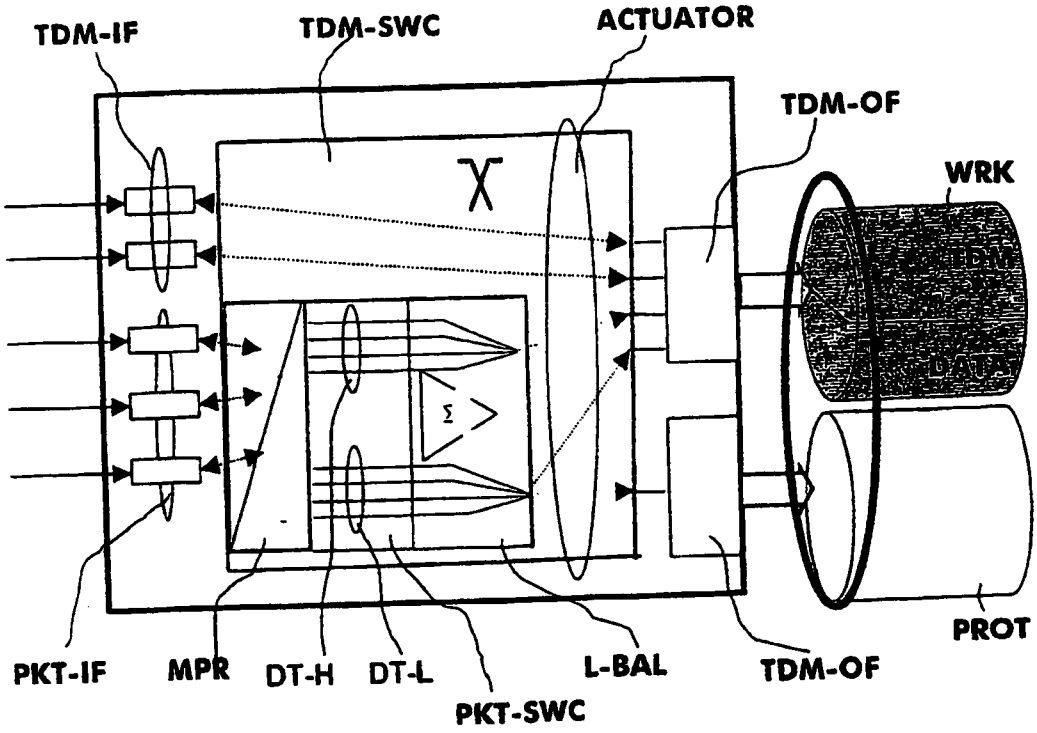
TDM-IF
TDM-SWC
ACTUATOR
TDM-OF
WRK
PROT
PKT-IF
MPR
DT-H
DT-L
PKT-SWC
L-BAL
TDM-OF

FIG. 6

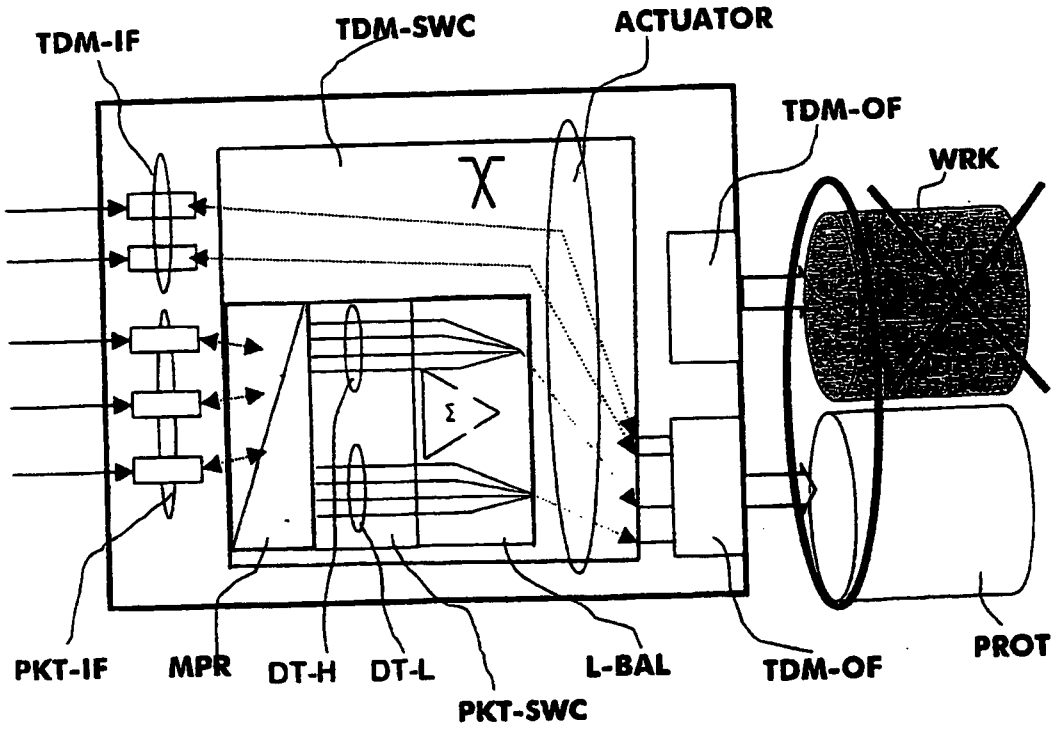
TDM-IF
TDM-SWC
ACTUATOR
TDM-OF
WRK
PROT
PKT-IF
MPR
DT-H
DT-L
PKT-SWC
L-BAL
TDM-OF

FIG. 7