(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2019-79288
(P2019-79288A)
(43)公開日　令和1年5月23日(2019.5.23)

(51)Int.Cl.		F I			テーマコード（参考）
G05B 23/02	(2006.01)	G05B	23/02	V	3C223
G08B 29/16	(2006.01)	G08B	29/16		5C087
G08B 29/02	(2006.01)	G08B	29/02		
H04B 1/74	(2006.01)	H04B	1/74		

審査請求 未請求　請求項の数 4　ＯＬ　（全 11 頁）

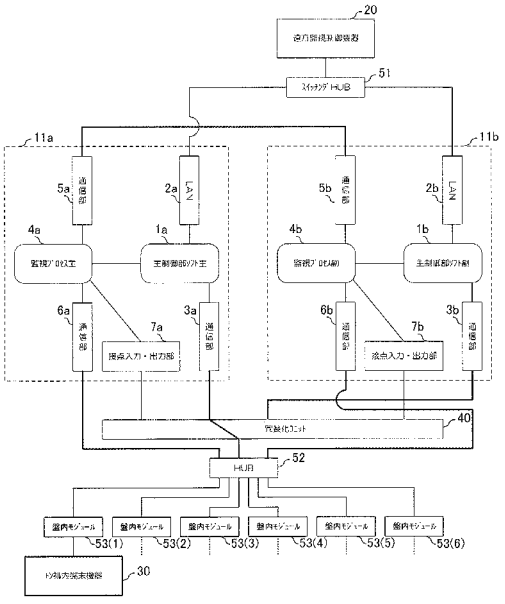
(21)出願番号　特願2017-205912 (P2017-205912)
(22)出願日　平成29年10月25日 (2017.10.25)

(71)出願人　000233826
能美防災株式会社
東京都千代田区九段南４丁目７番３号
(74)代理人　100110423
弁理士　曾我　道治
(74)代理人　100111648
弁理士　梶並　順
(74)代理人　100147566
弁理士　上田　俊一
(74)代理人　100161171
弁理士　吉田　潤一郎
(74)代理人　100188514
弁理士　松岡　隆裕
(74)代理人　100194939
弁理士　別所　公博

最終頁に続く

(54)【発明の名称】受信盤

(57)【要約】
【課題】故障発生時のシステムダウンを回避することができる適切な冗長構成を備えた受信盤を得る。
【解決手段】２重化された第１の制御装置と第２の制御装置と、いずれかの制御装置を選択切り換え可能な冗長化ユニットとを備えた受信盤であって、第２の制御装置は、端末装置の監視・制御を実行する主制御実行部と、通常運用中の第１の制御装置に異常が発生していないかを監視する監視部とを有し、監視部は、第１の制御装置が通常運用中に、通常運用時における監視・制御を実行中の制御装置に固定で割り当てられる制御ノードの存在が確認できない場合には、第１の制御装置に異常が発生したと判断し、冗長化ユニットを切り換え制御し、第２の制御装置により通常運用時における複数の端末装置の監視・制御を継続させる。
【選択図】図３



【特許請求の範囲】
【請求項１】
端末装置の監視・制御を実行するために２重化された第１の制御装置と第２の制御装置と、
前記第１の制御装置および前記第２の制御装置のいずれかに選択切り換えすることで、選択された制御装置により通常運用時における前記端末装置の監視・制御を実行させる冗長化ユニットと
を備えた受信盤であって、

前記第２の制御装置は、
前記端末装置の監視・制御を実行する主制御実行部と、
前記第１の制御装置が前記通常運用時における前記端末装置の監視・制御を実行している際に、前記第１の制御装置に異常が発生していないかを監視する監視部と
を有し、
前記第１の制御装置が前記通常運用時における監視・制御を実行している際に、前記監視部は、前記通常運用時における監視・制御を実行中の制御装置に固定で割り当てられる制御ノードの存在を確認し、前記制御ノードの存在が確認できない場合には、前記第１の制御装置に異常が発生したと判断し、前記第１の制御装置から前記第２の制御装置に選択切り換えするように前記冗長化ユニットを切り換え制御し、前記第２の制御装置により前記通常運用時における前記端末装置の監視・制御を継続させる
受信盤。
【請求項２】
端末装置の監視・制御を実行するために２重化された第１の制御装置と第２の制御装置と、
前記第１の制御装置および前記第２の制御装置のいずれかに選択切り換えすることで、選択された制御装置により通常運用時における前記端末装置の監視・制御を実行させる冗長化ユニットと
を備えた受信盤であって、
前記第２の制御装置は、
前記端末装置の監視・制御を実行する主制御実行部と、
前記第１の制御装置が前記通常運用時における前記端末装置の監視・制御を実行している際に、前記第１の制御装置に異常が発生していないかを監視する監視部と
を有し、
前記第１の制御装置が前記通常運用時における監視・制御を実行している際に、前記監視部は、前記第１の制御装置との通信が途絶えた場合には、前記第１の制御装置に異常が発生したと判断し、前記第１の制御装置から前記第２の制御装置に選択切り換えするように前記冗長化ユニットを切り換え制御し、前記第２の制御装置により前記通常運用時における前記端末装置の監視・制御を継続させる
受信盤。
【請求項３】
端末装置の監視・制御を実行するために２重化された第１の制御装置と第２の制御装置と、
前記第１の制御装置および前記第２の制御装置のいずれかに選択切り換えすることで、選択された制御装置により通常運用時における前記端末装置の監視・制御を実行させる冗長化ユニットと
を備えた受信盤であって、
前記第２の制御装置は、
前記端末装置の監視・制御を実行する主制御実行部と、
前記第１の制御装置が前記通常運用時における前記端末装置の監視・制御を実行している際に、前記第１の制御装置に異常が発生していないかを監視する監視部と

を有し、
前記第１の制御装置は、前記第１の制御装置が起動中に常時ＯＮとなるようなＯＮ接点信号を出力し、
前記第１の制御装置が前記通常運用時における監視・制御を実行している際に、前記監視部は、前記第１の制御装置から出力された前記ＯＮ接点信号を入力接点信号として読み取り、前記入力接点信号がＯＦＦである場合には、前記第１の制御装置に異常が発生したと判断し、前記第１の制御装置から前記第２の制御装置に選択切り換えするように前記冗長化ユニットを切り換え制御し、前記第２の制御装置により前記通常運用時における前記端末装置の監視・制御を継続させる
受信盤。
【請求項４】
端末装置の監視・制御を実行するために２重化された第１の制御装置と第２の制御装置と、
前記第１の制御装置および前記第２の制御装置のいずれかに選択切り換えすることで、選択された制御装置により通常運用時における前記端末装置の監視・制御を実行させる冗長化ユニットと
を備えた受信盤であって、
前記第２の制御装置は、
前記端末装置の監視・制御を実行する主制御実行部と、
前記第１の制御装置が前記通常運用時における前記端末装置の監視・制御を実行している際に、前記第１の制御装置に異常が発生していないかを監視する監視部と
を有し、
前記第１の制御装置が前記通常運用時における監視・制御を実行している際に、前記監視部は、
前記第１の制御装置との通信が途絶えた場合には、前記第１の制御装置に異常が発生したと判断し、前記第１の制御装置から前記第２の制御装置に選択切り換えするように前記冗長化ユニットを切り換え制御し、前記第２の制御装置により前記通常運用時における前記端末装置の監視・制御を継続させる第１の監視機能と、
前記通常運用時における監視・制御を実行中の制御装置に固定で割り当てられる制御ノードの存在を確認し、前記制御ノードの存在が確認できない場合には、前記第１の制御装置に異常が発生したと判断し、前記第１の制御装置から前記第２の制御装置に選択切り換えするように前記冗長化ユニットを切り換え制御し、前記第２の制御装置により前記通常運用時における前記端末装置の監視・制御を継続させる第２の監視機能と、
前記第１の制御装置は、前記第１の制御装置が起動中に常時ＯＮとなるようなＯＮ接点信号を出力し、
前記第１の制御装置が起動中に常時ＯＮとなる信号として前記第１の制御装置から出力されるＯＮ接点信号を入力接点信号として読み取り、前記入力接点信号がＯＦＦである場合には、前記第１の制御装置に異常が発生したと判断し、前記第１の制御装置から前記第２の制御装置に選択切り換えするように前記冗長化ユニットを切り換え制御し、前記第２の制御装置により前記通常運用時における前記端末装置の監視・制御を継続させる第３の監視機能
の３つの監視機能のうち、２つ以上の監視機能を有し、前記２つ以上の監視機能の組合せに基づいて、前記第１の制御装置に異常が発生していないかを監視する
受信盤。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、端末機器の監視・制御を行うとともに、上位装置との間で監視・制御に関する情報をやり取りする受信盤に関し、特に防災システムに用いられる防災受信盤に関する。

【背景技術】
【０００２】
自動車専用道路等のトンネルには、トンネル内で発生する火災事故から人身および車両を守るため、非常用施設が設置されている。このような非常用施設としては、火災の監視と通報のために火災検知器、手動通報装置、非常電話が設けられている。また、火災の消火および延焼防止のために、消火栓装置が設けられ、さらに、トンネル躯体およびダクト内を火災から防護するために、水噴霧ヘッドから消火用水を散水させる水噴霧設備などが設置される。
【０００３】
このように、トンネル内に設置された種々の端末機器を監視制御する防災受信盤を設けることで、トンネル防災システムを構築している従来技術がある（例えば、特許文献１参照）。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００２－２４６９６２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、従来技術には、以下のような課題がある。
トンネルの防災システムに適用されるトンネル防災受信盤は、主制御機能をパソコンが担っており、１台のパソコンにて運用している。パソコンとしては、連続稼働が可能な工業用のものが用いられる。
【０００６】
しかしながら、パソコンは、ハードディスク故障、マザーボード故障などのハードウェア故障、およびＯＳのフリーズ、アプリケーションエラーなどのソフトウェア故障、といった様々な故障が考えられる。なお、以下の説明において、このようなハードウェアの故障あるいはソフトウェアの故障がパソコンに発生した状態を、「異常発生時」と称することもある。このような異常発生時には、主制御機能を担っているパソコンがダウンすることになり、トンネル防災受信盤の機能が停止し、トンネル防災システムの運用に支障をきたす。
【０００７】
そして、このような異常発生時には、主制御部の修理、交換等を迅速に実施して対応していた。
【０００８】
本発明は、前記のような課題を解決するためになされたものであり、異常発生時のシステムダウンを回避することができる適切な冗長構成を備えた受信盤を得ることを目的とする。
【課題を解決するための手段】
【０００９】
本発明に係る受信盤は、端末装置の監視・制御を実行するために２重化された第１の制御装置と第２の制御装置と、第１の制御装置および第２の制御装置のいずれかに選択切り換えすることで、選択された制御装置により通常運用時における端末装置の監視・制御を実行させる冗長化ユニットとを備えた受信盤であって、第２の制御装置は、端末装置の監視・制御を実行する主制御実行部と、第１の制御装置が通常運用時における端末装置の監視・制御を実行している際に、第１の制御装置に異常が発生していないかを監視する監視部とを有し、第１の制御装置が通常運用時における監視・制御を実行している際に、監視部は、第１の制御装置との通信が途絶えた場合には、第１の制御装置に異常が発生したと判断し、第１の制御装置から第２の制御装置に選択切り換えするように冗長化ユニットを切り換え制御し、第２の制御装置により通常運用時における端末装置の監視・制御を継続

させる第１の監視機能と、通常運用時における監視・制御を実行中の制御装置に固定で割り当てられる制御ノードの存在を確認し、制御ノードの存在が確認できない場合には、第１の制御装置に異常が発生したと判断し、第１の制御装置から第２の制御装置に選択切り換えするように冗長化ユニットを切り換え制御し、第２の制御装置により通常運用時における端末装置の監視・制御を継続させる第２の監視機能と、第１の制御装置は、第１の制御装置が起動中に常時ＯＮとなるようなＯＮ接点信号を出力し、第１の制御装置が起動中に常時ＯＮとなる信号として第１の制御装置から出力されるＯＮ接点信号を入力接点信号として読み取り、入力接点信号がＯＦＦである場合には、第１の制御装置に異常が発生したと判断し、第１の制御装置から第２の制御装置に選択切り換えするように冗長化ユニットを切り換え制御し、第２の制御装置により通常運用時における端末装置の監視・制御を継続させる第３の監視機能の３つの監視機能のうち、少なくともいずれか１つの監視機能を有するものである。

【発明の効果】

【００１０】

本発明によれば、通常運用として動作している主制御部パソコンに異常が発生したことを、３種の監視機能の少なくとも１つに基づいて判断でき、異常発生時においても、バックアップ用の主制御部パソコンに切り換えることで、システムの継続運転を可能とする構成を備えている。この結果、異常発生時のシステムダウンを回避することができる適切な冗長構成を備えた受信盤を得ることができる。

【図面の簡単な説明】

【００１１】

【図１】主制御部パソコンが冗長化されていない従来のトンネル防災システムの概略構成を示す説明図である。

【図２】本発明の実施の形態１に係る、主制御部パソコンが冗長化されたトンネル防災システムの概略構成を示す説明図である。

【図３】本発明の実施の形態１に係る、主制御部パソコンが冗長化されたトンネル防災システムの詳細構成を示す説明図である。

【発明を実施するための形態】

【００１２】

以下、本発明の受信盤につき、図面を用いて説明する。

本発明は、主制御部パソコンを２重化した際に、それぞれの主制御部パソコンが、相手側の主制御部パソコンの状態を３種類の手法の少なくともいずれか１つの手法により監視することで、種々の異常発生に対し、システムがダウンすることを回避し、監視・制御の継続を可能とすることを技術的特徴とするものである。そこで、このような技術的特徴を備えた受信盤について、特に、トンネル内の火災等を監視する防災受信盤を具体例として、実施の形態を用いて、以下に詳細に説明する。

【００１３】

実施の形態１．

本発明の具体的な構成を説明する前に、従来技術である防災受信盤の概略構成と、本発明に係る防災受信盤の概略構成を、図面を用いて説明する。なお、以下の説明では、防災受信盤に組み込まれ、システムの監視・制御を実行する構成を、「主制御部パソコン」と称することとする。

【００１４】

図１は、主制御部パソコンが冗長化されていない従来のトンネル防災システムの概略構成を示す説明図である。一般的に、防災受信盤１１０は、各トンネルに１つ設けられ、接続される複数の端末機器３０によってトンネル内を監視している。遠方監視制御装置２０は、複数のトンネルの状況を確認するものであり、複数の防災受信盤１１０と接続されている。図１に示す従来のトンネル防災システムの例では、遠方監視制御装置２０と、トンネル内の各端末機器３０との間に、１台の主制御部パソコン１１１を有する防災受信盤１１０が設けられているものとして説明する。

【００１５】
このような構成において、主制御部パソコン１１に何らかのハードウェア故障あるいはソフトウェア故障が発生してしまうと、トンネル内の各端末機器３０の監視・制御が実施できず、システムダウンとなり、トンネル内が無監視状態となる。
【００１６】
これに対して、図２は、本発明の実施の形態１に係る、主制御部パソコンが冗長化されたトンネル防災システムの概略構成を示す説明図である。図２に示した本実施の形態１に係るトンネル防災システムは、図１に示した従来のトンネル防災システムにおける防災受信盤１１０の代わりに、防災受信盤１０を備えている。すなわち、図２に示す本実施の形態１に係るトンネル防災システムは、遠方監視制御装置２０と、トンネル内の各端末機器３０との間に、冗長化された２台の制御装置としての主制御部パソコン１１ａ、１１ｂを有する防災受信盤１０が設けられている。
【００１７】
図２の構成を備えたトンネル防災システムは、主制御部パソコン１１ａが何らかの故障によりダウンした場合にも、バックアップ用の主制御部パソコン１１ｂに切り換えることにより、システムの継続運転が可能となっている。
【００１８】
このような切り換えを実現するために、本実施の形態１に係る受信盤は、通常運用中の主制御部パソコンが正常に機能しているかを、バックアップ側の主制御部パソコンがソフトウェア的に監視する機能を備えている点を技術的特徴としている。そこで、主制御部パソコン１１ａ、１１ｂの具体的な内部構成およびソフトウェア処理について、図３を用いて詳細に説明する。
【００１９】
図３は、本発明の実施の形態１に係る、主制御部パソコンが冗長化されたトンネル防災システムの詳細構成を示す説明図である。図２に示す本実施の形態１に係るトンネル防災システムは、２台の主制御部パソコン１１ａ、１１ｂ、遠方監視制御装置２０、トンネル内端末機器３０、および冗長化ユニット４０を主な構成としている。
【００２０】
遠方監視制御装置２０と、２台の主制御部パソコン１１ａ、１１ｂとは、スイッチングＨＵＢ５１を介して相互通信が可能となっている。また、冗長化ユニット４０は、２台の主制御部パソコン１１ａ、１１ｂのいずれか１台と、選択的にハードウェア接続されるように、主制御部パソコン１１内の監視プロセス４によって制御される。主制御部パソコン１１の内部構成の詳細については、後述する。
【００２１】
冗長化ユニット４０と接続された主制御部パソコン１１ａまたは主制御部パソコン１１ｂと、各トンネル内端末機器３０と通信を行う盤内モジュール５３（ｎ）とは、受信盤１０内の通信を行うための通信プロトコルを備えるＨＵＢ５２を介して相互通信が可能となっている。この結果、主制御部パソコン１１ａ、１１ｂは、冗長化ユニット４０、ＨＵＢ５２、および盤内モジュール５３（ｎ）を経由することで、各トンネル内端末機器３０の監視・制御を実行する。なお、受信盤１０内の通信を行うための通信プロトコルは、アークネットやイーサネット（登録商標）等が適用でき、本発明において通信プロトコルは、特に限定されない。
なお、図３では、盤内モジュール５３（ｎ）として、ノードＩＤ１～６に相当する６台の盤内モジュール５３（１）～盤内モジュール５３（６）を有している場合を例示している。
【００２２】
次に、冗長化機能を実行する主制御部パソコン１１ａ、１１ｂの構成・機能について、詳細に説明する。主制御部パソコン１１ａは、主制御部ソフト１ａ、ＬＡＮ２ａ、通信部３ａ、監視プロセス４ａ、通信部５ａ、通信部６ａ、および接点入力・出力部７ａを備えて構成されている。同様に、主制御部パソコン１１ｂは、主制御部ソフト１ｂ、ＬＡＮ２

ｂ、通信部３ｂ、監視プロセス４ｂ、通信部５ｂ、通信部６ｂ、および接点入力・出力部７ｂを備えて構成されている。

【００２３】

このように、主制御部パソコン１１ａと主制御部パソコン１１ｂは、いずれか一方が通常の運用時に動作している際に、他方がバックアップとして機能できるように、同様の構成を備えている。そこで、以下では、１台目の主制御部パソコン１１ａが、通常の運用時に動作している制御装置（第１の制御装置に相当）であり、２台目の主制御部パソコン１１ｂ（第２の制御装置に相当）が、バックアップ用として待機している制御装置であるとして、動作説明する。

【００２４】

なお、図３では、１台目の主制御部パソコン１１ａが、通常の運用時に動作している第１の制御装置であるため、主制御部ソフト１ａ（第１の主制御実行部に相当）を「主制御部ソフト主」と表記し、監視プロセス４ａを「監視プロセス主」と表記している。同様に、図３では、２台目の主制御部パソコン１１ｂが、バックアップ用として待機している第２の制御装置であるため、主制御部ソフト１ｂ（第２の主制御実行部に相当）を「主制御部ソフト副」と表記し、監視プロセス４ｂを「監視プロセス副」と表記している。

【００２５】

主制御部ソフト１ａは、通常の運用時にトンネル内端末機器３０の監視・制御を行うためのソフトウェアを実行する主制御実行部である。具体的には、主制御部ソフト１ａは、ＬＡＮ２ａを介して、遠方監視制御装置２０と監視・制御に関連する情報を相互通信する。また、主制御部ソフト１ａは、通信部３ａを介して、各トンネル内端末機器３０と監視・制御に関連する情報を相互通信する。

【００２６】

従って、主制御部ソフト１ａ、ＬＡＮ２ａ、および通信部３ａは、冗長化機能を有していない従来の主制御部パソコン１１にも備わっており、監視・制御を実行するために標準装備された構成に相当する。

【００２７】

一方、監視プロセス４ａ、通信部５ａ、通信部６ａ、および接点入力・出力部７ａは、冗長化機能を実現するために、主制御部パソコン１１ａ内に新たに装備された構成に相当する。同様に、監視プロセス４ｂ、通信部５ｂ、通信部６ｂ、および接点入力・出力部７ｂは、冗長化機能を実現するために、主制御部パソコン１１ｂ内に新たに装備された構成に相当する。

【００２８】

監視プロセス４ａは、監視プロセス４ｂと協働しながら、監視プロセス４ｂを経由して、自身の主制御部ソフト１ａと、相手方の主制御部ソフト１ｂおよび監視プロセス４ｂが正常に動作しているか否かを監視するソフトウェアを実行する監視部である。同様に、監視プロセス４ｂは、監視プロセス４ａと協働しながら、監視プロセス４ａを経由して、自身の主制御部ソフト１ｂと、相手方の主制御部ソフト１ａおよび監視プロセス４ａが正常に動作しているか否かを監視するソフトウェアを実行する監視部である。

【００２９】

通信部５ａおよび通信部５ｂは、監視プロセス４ａと監視プロセス４ｂとが相互通信を行うための通信インターフェースである。

【００３０】

通信部６ｂは、主制御部パソコン１１ｂがバックアップ用として動作している際に、ＨＵＢ５２を介して監視プロセス４ｂが特定のノードの存在を監視することを可能とさせるための通信インターフェースである。

【００３１】

また、通信部６ａは、主制御部パソコン１１ａがバックアップ用として動作する際に、ＨＵＢ５２を介して監視プロセス４ａが特定のノード（後述する通信部３ａ、３ｂのノード２５５）の存在を監視することを可能とさせるための通信インターフェースである。

【００３２】
監視プロセス４ａ、４ｂ（通信部６ａ、６ｂ）を用いた主制御部ソフト１ａ、１ｂ（通信部３ａ、３ｂ）の監視機能の詳細は、後述する。
【００３３】
接点入力・出力部７ａおよび接点入力・出力部７ｂは、監視プロセス４ａと監視プロセス４ｂとが相互に主制御部パソコン１１ａ、１１ｂの接点入出力を確認するための入出力部である。
【００３４】
本実施の形態１では、主制御部パソコン１１ａに含まれている監視プロセス４ａが通信部５ａ、通信部６ａ、および接点入力・出力部７ａを介して、また、主制御部パソコン１１ｂに含まれている監視プロセス４ｂが通信部５ｂ、通信部６ｂ、および接点入力・出力部７ｂを介して、主制御部パソコン１１ａが故障によりダウンした場合に、バックアップ用の主制御部パソコン１１ｂに切り換えるための３つの監視機能を実現している。そこで、これら３つの監視機能について、以下に詳述する。
【００３５】
［第１の監視機能］通信部５ａ、５ｂを用いた監視機能
通信部５ａ、５ｂにより、監視プロセス主４ａと監視プロセス副４ｂで相互通信を行うことで、監視プロセス４ａ、４ｂは、お互いに生存確認（ソフトの停止、異常の確認）を行う。そして、相手との通信が途絶えた場合には、相手方のパソコン故障と見なし、バックアップ用として待機しているパソコンへ切り換えることが可能となる。
【００３６】
図３に示した構成例では、バックアップとして待機している監視プロセス４ｂは、通信部５ｂ、通信部５ａを介して、通常運用として動作している主制御部パソコン１１ａ内の監視プロセス４ａと通信を行うことで、主制御部パソコン１１ａの生存確認（詳細には、監視プロセス４ａのソフトの停止等の異常確認）を行う。そして、監視プロセス４ｂは、監視プロセス４ａとの通信が途絶えた場合には、主制御部パソコン１１ａが故障した（詳細には、監視プロセス４ａが故障した）と判断する。
【００３７】
監視プロセス４ｂは、主制御部パソコン１１ａが故障したと判断した場合には、バックアップ用として待機している自身の主制御部パソコン１１ｂにより監視・制御を実行するために、冗長化ユニット４０の切り換えを実行する。この結果、主制御部パソコン１１ａが故障し、通信部５ａ、５ｂを介した相互通信が不可能になった場合にも、バックアップ用の主制御部パソコン１１ｂにより、システムの継続運転が可能である。
【００３８】
［第２の監視機能］通信部６ａ、６ｂを用いた監視機能
盤内モジュール５３（ｎ）との通信において、監視・制御を実行中の主制御部ソフト１（すなわち、主制御部ソフト１ａまたは主制御部ソフト１ｂの両方）に特定の制御ノード（例えば、ノードＩＤ２５５）を固定して割り当ててある。そして、冗長化ユニット４０により、主制御部ソフト１ａまたは主制御部ソフト１ｂは、どちらか一方しか、冗長化ユニット４０を介した盤内モジュール５３（ｎ）との通信経路に存在しないようになっている。存在するのは、運用中の主制御部ソフト１である。
【００３９】
そこで、バックアップとして待機している監視プロセス４ｂは、通信部６ｂを介してＨＵＢ５２を経由し、主制御部ソフト１ａのノードＩＤ２５５の存在を常時監視する。そして、監視プロセス４ｂは、ノードＩＤ２５５の存在が確認できなくなった場合には、主制御部ソフト１ａの停止等の異常や主制御部パソコン１１ａの異常が発生したと判断する。
【００４０】
監視プロセス４ｂは、主制御部ソフト１ａの異常や主制御部パソコン１１ａの異常が発生したと判断した場合には、バックアップ用として待機している自身の主制御部パソコン１１ｂにより監視・制御を実行するために、冗長化ユニット４０の切り換えを実行する。

この結果、主制御部ソフト１ａの異常や主制御部パソコン１１ａの異常により、主制御部ソフト１ａのノードＩＤ２５５の存在確認ができなくなった場合にも、バックアップ用の主制御部パソコン１１ｂにより、システムの継続運転が可能である。

【００４１】

［第３の監視機能］接点入力・出力部７ａ、７ｂを用いた監視機能

主制御部パソコン１１ａ内の接点入力・出力部７ａからの接点出力は、冗長化ユニット４０を介して、主制御部パソコン１１ｂ内の接点入力・出力部７ｂの接点入力に接続されている。同様に、主制御部パソコン１１ｂ内の接点入力・出力部７ｂからの接点出力は、冗長化ユニット４０を介して、主制御部パソコン１１ａ内の接点入力・出力部７ａの接点入力に接続されている。

【００４２】

このような接続を用いて、監視プロセス４ａ、４ｂは、お互いに接点入出力に基づく生存確認を行う。具体的には、監視プロセス４ａ、４ｂは、自身のパソコンが起動している際には接点出力をＯＮ状態とする。この結果、監視プロセス４ａ、４ｂは、相手方からの接点出力がＯＮ状態であるか否かを接点入力として確認し、接点入力がＯＦＦになった場合には、相手方のパソコンが故障したと判断できる。

【００４３】

図３に示した構成例では、バックアップとして待機している監視プロセス４ｂは、接点入力・出力部７ｂ、冗長化ユニット４０、および接点入力・出力部７ａを介して、監視プロセス４ａからの接点入力がＯＮ状態であるか否かを確認する。そして、監視プロセス４ｂは、監視プロセス４ａからの接点入力がＯＦＦとなった場合には、主制御部パソコン１１ａが故障したと判断する。

【００４４】

監視プロセス４ｂは、主制御部パソコン１１ａが故障したと判断した場合には、バックアップ用として待機している自身の主制御部パソコン１１ｂにより監視・制御を実行するために、冗長化ユニット４０の切り換えを実行する。この結果、主制御部パソコン１１ａが故障し、接点入出力が正常に読み取れなくなった場合にも、バックアップ用の主制御部パソコン１１ｂにより、システムの継続運転が可能である。

【００４５】

以上のように、実施の形態１によれば、通常運用として動作している主制御部パソコンに故障が発生したことを、監視プロセス４による３種の監視機能に基づいて判断できる構成を備えている。従って、バックアップとして待機している主制御部パソコン１１は、３種の監視機能の少なくともいずれか１つで故障が検出された場合には、バックアップ用の主制御部パソコン１１に切り換えることで、システムの継続運転を可能としている。そして、通常運用していた主制御部パソコン１１が故障したことを遠方監視制御装置２０に送信する。

【００４６】

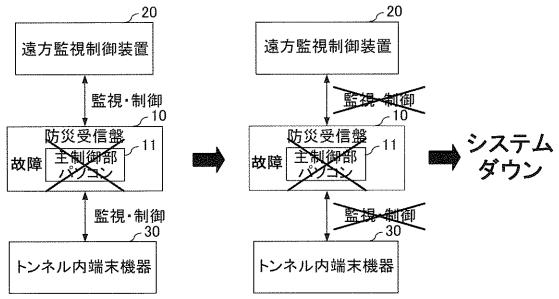
なお、本実施の形態では、防災受信盤１０がトンネル内端末機器３０と接続されているシステムで説明したが、トンネルの規模が大きくなれば、防災受信盤１０は、中継盤を介してトンネル内端末機器３０と接続されることになる。この場合、中継盤の冗長化の構成は、防災受信盤１０と同様であり、防災受信盤１０および中継盤が冗長化される。

【００４７】

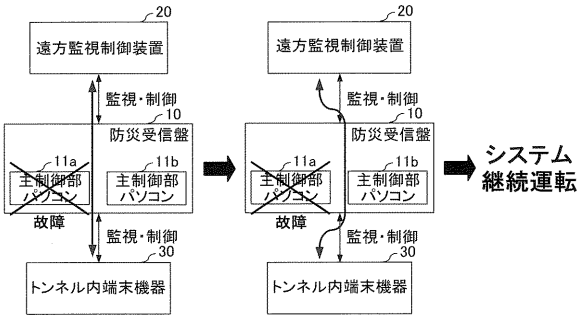
従来は、ハードディスクだけは、ミラー構成により２重化されていた。これに対して、本発明では、上述した３種の監視機能を実行する構成をさらに備えている。この結果、通常運用として動作している主制御部パソコンに関して、監視ソフトが停まってしまった異常検出を第１の監視機能で実現し、主制御部ソフトだけが停まってしまった異常検出を第２の監視機能で実現し、ハードウェア自体の故障検出を第３の監視機能で実現している。なお、ハードウェアの故障は、第１の監視機能、第２の監視機能でも検出することができる。従って、想定される種々の故障に対して、故障発生時のシステムダウンを回避することができる適切な冗長構成を備えた受信盤を実現できる。

【００４８】
また、第１～３の監視機能は、それぞれで異常を検出するのではなく、組合せで検出する異常もある。例えば、通信部５ａ、５ｂ間の線が断線した場合、第１の監視機能によれば両方の監視プロセス４ａ、４ｂが異常だと検出してしまう。そこで、通信部５ａ、５ｂ間の断線を第１の監視機能と第２の監視機能の組み合わせで監視することで、通信部５ａ、５ｂ間の通信が途絶えても、監視プロセス４ｂは、ノードＩＤ２５５の存在が確認できている場合には、主制御部パソコン１１ａはシステムを監視できるとして主制御部パソコン１１ｂは自身に切り換えることはせず、断線異常を警報する。
【００４９】
また、第１または第２の監視機能で検出する主制御部ソフトだけが停まってしまった異常が発生した場合、バックアップ用の主制御部パソコン１１から通常運用していて異常が発生した主制御部パソコン１１に再起動の信号を出力し、ソフトの異常を解消しても良い。
【符号の説明】
【００５０】
１ａ、１ｂ　主制御部ソフト、２ａ、２ｂ　ＬＡＮ、３ａ、３ｂ　通信部、４ａ、４ｂ　監視プロセス、５ａ、５ｂ　通信部、６ａ、６ｂ　通信部、７ａ、７ｂ　接点入力・出力部、１０　防災受信盤、１１ａ、１１ｂ　主制御部パソコン、２０　遠方監視制御装置、３０　トンネル内端末機器、４０　冗長化ユニット、５１　スイッチングＨＵＢ、５２　ＨＵＢ、５３　盤内モジュール。

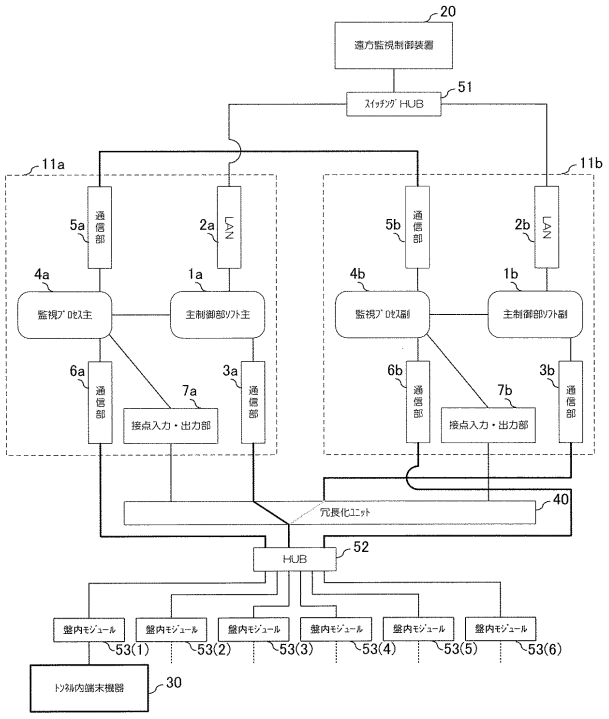
【図１】



【図２】



【図３】



フロントページの続き

(74)代理人 100206782
弁理士 佐藤 彰洋
(72)発明者 大西 和之
東京都千代田区九段南４丁目７番３号 能美防災株式会社内
(72)発明者 狩山 則之
東京都千代田区九段南４丁目７番３号 能美防災株式会社内
(72)発明者 佐々木 建弥
東京都千代田区九段南４丁目７番３号 能美防災株式会社内

Ｆターム(参考) 3C223 AA15 BA03 BA05 CC02 CC06 DD03 DD06 EA01 GG01
5C087 BB74 CC02 CC22 CC42 CC46 DD04 DD28 EE08 EE19 FF01
FF02 FF03 FF04 FF19 GG54