(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2018-190081
(P2018-190081A)
(43)公開日　平成30年11月29日(2018.11.29)

(51)Int.Cl.		F I		テーマコード（参考）
G05B 9/03	(2006.01)	G05B	9/03	5H209

審査請求 未請求　請求項の数 10　ＯＬ　（全 15 頁）

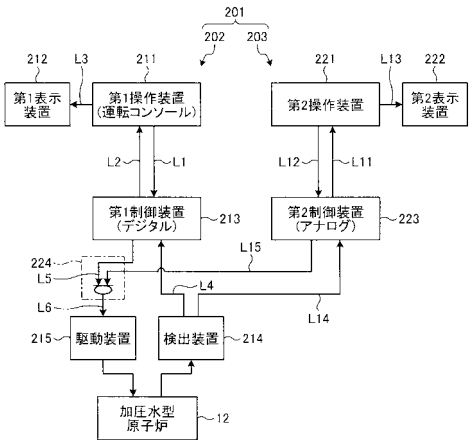
(21)出願番号　特願2017-90413(P2017-90413)
(22)出願日　平成29年4月28日(2017.4.28)

(71)出願人　000006208
三菱重工業株式会社
東京都港区港南二丁目１６番５号
(74)代理人　110002147
特許業務法人酒井国際特許事務所
(72)発明者　白澤　寛司
東京都港区港南二丁目１６番５号　三菱重工業株式会社内
(72)発明者　石本　俊輔
東京都港区港南二丁目１６番５号　三菱重工業株式会社内
(72)発明者　金杉　将幸
東京都港区港南二丁目１６番５号　三菱重工業株式会社内

Ｆターム(参考)　5H209 AA03　SS01　SS05　SS08　TT04　TT05

(54)【発明の名称】プラントの監視制御装置

(57)【要約】
【課題】プラントの監視制御装置において、サイバー攻撃により制御装置によるプラント制御の健全性が損なわれてもプラントの安全性を維持することができる。
【解決手段】原子力発電プラント１０の運転状態が入力されると共にプラント機器に対して駆動制御信号を出力する第１制御装置２１３と、第１制御装置２１３に対して電気的に独立して設けられて原子力発電プラント１０の運転状態が入力されると共にプラント機器に対して駆動制御信号を出力する第２制御装置２２３と、第１制御装置２１３からの駆動制御信号よりも第２制御装置２２３からの駆動制御信号を優先的にプラント機器に出力する切替装置２２４とを備えている。
【選択図】図１



【特許請求の範囲】
【請求項１】
プラントの運転状態が入力されると共にプラント機器に対して駆動制御信号を出力する第１制御装置と、
前記第１制御装置に対して電気的に独立して設けられて前記プラントの運転状態が入力されると共に前記プラント機器に対して駆動制御信号を出力する第２制御装置と、
前記第１制御装置からの駆動制御信号よりも前記第２制御装置からの駆動制御信号を優先的に前記プラント機器に出力する切替装置と、
を備えることを特徴とするプラントの監視制御装置。
【請求項２】
前記第２制御装置は、入力される前記プラントの運転状態に基づいてプラントの異常発生を検出したときに前記プラント機器に対して駆動制御信号を出力することを特徴とする請求項１に記載のプラントの監視制御装置。
【請求項３】
前記切替装置は、前記第２制御装置からの駆動制御信号の入力がないときに前記第１制御装置からの駆動制御信号を前記プラント機器に出力し、前記第２制御装置からの駆動制御信号の入力があるときに前記第２制御装置からの駆動制御信号を前記プラント機器に出力することを特徴とする請求項１または請求項２に記載のプラントの監視制御装置。
【請求項４】
前記切替装置は、前記第２制御装置からの駆動制御信号の入力があるときに、前記第１制御装置からの駆動制御信号を遮断して前記第２制御装置からの駆動制御信号を前記プラント機器に出力するＯＲ回路であることを特徴とする請求項３に記載のプラントの監視制御装置。
【請求項５】
前記第１制御装置は、駆動制御信号としてのデジタル信号を出力し、前記第２制御装置は、駆動制御信号としてのアナログ信号を出力することを特徴とする請求項１から請求項４のいずれか一項に記載のプラントの監視制御装置。
【請求項６】
前記第２制御装置は、書き換え不能なマイクロプロセッサを有することを特徴とする請求項１から請求項５のいずれか一項に記載のプラントの監視制御装置。
【請求項７】
前記第２制御装置は、前記プラントの運転状態を検出する検出装置と前記プラント機器とがハードワイヤードにより接続されることを特徴とする請求項１から請求項６のいずれか一項に記載のプラントの監視制御装置。
【請求項８】
前記第２制御装置は、前記第１制御装置よりも前記プラント機器を駆動する機能が制限されることを特徴とする請求項１から請求項７のいずれか一項に記載のプラントの監視制御装置。
【請求項９】
前記第１制御装置は、前記プラントの起動操作、運転操作、停止操作を行うものであり、前記第２制御装置は、前記プラントの停止操作だけを行うものであることを特徴とする請求項８に記載のプラントの監視制御装置。
【請求項１０】
前記第２制御装置は、プラントの運転状態を表示する表示装置と、前記第２制御装置に操作信号を入力する操作装置が接続されることを特徴とする請求項１から請求項９のいずれか一項に記載のプラントの監視制御装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、プラントの異常が発生したとき、このプラントを安定させるための機能を有

するプラントの監視制御装置に関するものである。
【背景技術】
【０００２】
例えば、加圧水型原子炉（ＰＷＲ：Pressurized Water Reactor）を有する原子力発電プラントは、軽水を原子炉冷却材及び中性子減速材として使用し、原子炉の炉心全体にわたって沸騰しない高温高圧水とし、この高温高圧水を蒸気発生器に送って熱交換により蒸気を発生させ、この蒸気をタービン発電機へ送って発電するものである。そして、蒸気発生器は、原子炉からの高温高圧の一次系冷却水の熱を二次系冷却水に伝え、二次系冷却水で水蒸気を発生させるものである。
【０００３】
このような原子力発電プラントにて、原子炉は、中央制御室に配置された計装制御システムにより制御されている。この計装制御システムは、運転員がプラントの運転監視を行う中央制御盤が設けられ、この中央制御盤は、プラントのプロセス量を計測してポンプや弁などの補機を制御する常用系の装置と、プラントの異常時にこのプラントを安全に停止させる安全保護系の装置から構成されている。このような計装制御システムがサイバー攻撃を受けて乗っ取られると、悪意を持った操作などによる原子炉の安全性を確保することが困難となる。
【０００４】
このようなプラントへのサイバー攻撃に対する防衛として、計装制御システムのセキュリティレベルを上げることが考えられる。このような技術として、例えば、下記特許文献１に記載されたものがある。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２０１６－１２９３４６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
上述したように、計装制御システムのセキュリティレベルを上げることで、プラントへのサイバー攻撃に対する対策を講じることも必要であるが、この対策は、サイバー攻撃による計装制御システムへの侵入を検出し、この侵入を防止するものであり、一旦、計装制御システムへ侵入されてしまうと、悪意を持った操作などによる原子炉の安全性を確保することが困難となる。
【０００７】
本発明は、上述した課題を解決するものであり、サイバー攻撃により制御装置によるプラント制御の健全性が損なわれても、プラントの安全性を維持することができるプラントの監視制御装置を提供することを目的とする。
【課題を解決するための手段】
【０００８】
上記の目的を達成するための本発明のプラントの監視制御装置は、プラントの運転状態が入力されると共にプラント機器に対して駆動制御信号を出力する第１制御装置と、前記第１制御装置に対して電気的に独立して設けられて前記プラントの運転状態が入力されると共に前記プラント機器に対して駆動制御信号を出力する第２制御装置と、前記第１制御装置からの駆動制御信号よりも前記第２制御装置からの駆動制御信号を優先的に前記プラント機器に出力する切替装置と、を備えることを特徴とするものである。
【０００９】
従って、第２制御装置が第１制御装置に対して電気的に独立して設けられており、切替装置により第２制御装置からの駆動制御信号が第１制御装置からの駆動制御信号よりも優先的にプラント機器に出力されることから、例えば、サイバー攻撃により第１制御装置によるプラント制御の健全性が損なわれても、第１制御装置に代わって第２制御装置が優先

的にプラント機器を制御することとなり、プラントの安全性を維持することができる。

【００１０】

本発明のプラントの監視制御装置では、前記第２制御装置は、入力される前記プラントの運転状態に基づいてプラントの異常発生を検出したときに前記プラント機器に対して駆動制御信号を出力することを特徴としている。

【００１１】

従って、プラントの正常時は、第１制御装置がプラントの運転状態に基づいた駆動制御信号をプラント機器に出力し、プラントの異常発生は、第２制御装置がプラントの運転状態に基づいた駆動制御信号をプラント機器に出力することで、第１制御装置がサイバー攻撃により乗っ取られても、第２制御装置がプラント機器を安全に制御することができる。

【００１２】

本発明のプラントの監視制御装置では、前記切替装置は、前記第２制御装置からの駆動制御信号の入力がないときに前記第１制御装置からの駆動制御信号を前記プラント機器に出力し、前記第２制御装置からの駆動制御信号の入力があるときに前記第２制御装置からの駆動制御信号を前記プラント機器に出力することを特徴としている。

【００１３】

従って、プラントの正常時は、切替装置に第２制御装置からの駆動制御信号の入力がないことから、第１制御装置がプラントの運転状態に基づいてプラント機器を制御し、第１制御装置がサイバー攻撃によりプラントを不安定にさせる駆動制御信号を出力したとき、第２制御装置がプラントを安定させる駆動制御信号を出力し、切替装置は、第２制御装置の駆動制御信号をプラント機器に出力することで、第２制御装置がプラント機器を安全に制御することができる。

【００１４】

本発明のプラントの監視制御装置では、前記切替装置は、前記第２制御装置からの駆動制御信号の入力があるときに、前記第１制御装置からの駆動制御信号を遮断して前記第２制御装置からの駆動制御信号を前記プラント機器に出力するＯＲ回路であることを特徴としている。

【００１５】

従って、第１制御装置がサイバー攻撃によりプラントを不安定にさせる駆動制御信号を出力したとき、第２制御装置がプラントを安定させる駆動制御信号を出力し、切替装置としてのＯＲ回路は、第１制御装置からの駆動制御信号を遮断し、第２制御装置からの駆動制御信号をプラント機器に出力するため、第２制御装置の駆動制御信号によりプラント機器を安全に制御することができる。

【００１６】

本発明のプラントの監視制御装置では、前記第１制御装置は、駆動制御信号としてのデジタル信号を出力し、前記第２制御装置は、駆動制御信号としてのアナログ信号を出力することを特徴としている。

【００１７】

従って、第２制御装置は、第１制御装置が取り扱うデジタル信号と異なる形式のアナログ信号を用いることで、サイバー攻撃により第１制御装置にコンピュータウイルスが侵入しても、第２制御装置まで感染することが抑制され、第２制御装置によりプラント機器を安全に制御することができる。

【００１８】

本発明のプラントの監視制御装置では、前記第２制御装置は、前記第１制御装置に対するサイバー攻撃により影響を受けない回路を有することを特徴としている。

【００１９】

従って、第２制御装置が第１制御装置に対するサイバー攻撃により影響を受けない回路を有することで、サイバー攻撃により第１制御装置にコンピュータウイルスが侵入しても、コンピュータウイルスにより第２制御装置の回路が書き換えられることがなく、第２制御装置によりプラント機器を安全に制御することができる。

【００２０】
本発明のプラントの監視制御装置では、前記第２制御装置は、前記プラントの運転状態を検出する検出装置と前記プラント機器とがハードワイヤードにより接続されることを特徴としている。
【００２１】
従って、第２制御装置と検出装置とプラント機器とがハードワイヤードにより接続されることで、ネットワークからのサイバー攻撃を受けることがなく、第２制御装置によりプラント機器を安全に制御することができる。
【００２２】
本発明のプラントの監視制御装置では、前記第２制御装置は、前記第１制御装置よりも前記プラント機器を駆動する機能が制限されることを特徴としている。
【００２３】
従って、第２制御装置の機能は、第１制御装置の機能よりも縮小されることで、第２制御装置の設置による製造コストの増加を抑制することができる。
【００２４】
本発明のプラントの監視制御装置では、前記第１制御装置は、前記プラントの起動操作、運転操作、停止操作を行うものであり、前記第２制御装置は、前記プラントの停止操作だけを行うものであることを特徴としている。
【００２５】
従って、第１制御装置がプラントの起動操作、運転操作、停止操作を行うことから、プラントの正常時にプラント機器を正常に運転することができ、第２制御装置がプラントの停止操作だけを行うことから、第１制御装置によるプラントの制御が異常であるとき、第２制御装置がプラントを安全に停止させることができる。
【００２６】
本発明のプラントの監視制御装置では、前記第２制御装置は、プラントの運転状態を表示する表示装置と、前記第２制御装置に操作信号を入力する操作装置が接続されることを特徴としている。
【００２７】
従って、プラントの異常発生時に、表示装置にプラントの運転状態が表示されることから、オペレータは、操作装置を用いて第２制御装置に操作信号を出力し、第２制御装置によりプラントを安全に運転することができる。
【発明の効果】
【００２８】
本発明のプラントの監視制御装置によれば、サイバー攻撃により制御装置によるプラント制御の健全性が損なわれても、プラントの安全性を維持することができる。
【図面の簡単な説明】
【００２９】
【図１】図１は、本実施形態の原子力発電プラントの監視制御装置を表す概略構成図である。
【図２】図２は、本実施形態の原子力発電プラントの監視制御装置の動作を表すフローチャートである。
【図３】図３は、原子力発電プラントを表す概略構成図である。
【発明を実施するための形態】
【００３０】
以下に添付図面を参照して、本発明のプラントの監視制御装置の好適な実施形態を詳細に説明する。なお、この実施形態により本発明が限定されるものではなく、また、実施形態が複数ある場合には、各実施形態を組み合わせて構成するものも含むものである。
【００３１】
図３は、原子力発電プラントを表す概略構成図である。
【００３２】

本実施形態において、図３に示すように、原子力発電プラント１０は、原子炉を有している。この原子炉は、軽水を原子炉冷却材及び中性子減速材として使用し、炉心全体にわたって沸騰しない高温高圧水とし、この高温高圧水を後述する蒸気発生器に送って熱交換により蒸気を発生させ、この蒸気をタービン発電機へ送って発電する加圧水型原子炉（ＰＷＲ：Pressurized Water Reactor）である。なお、原子炉は、沸騰水型原子炉（ＢＷＲ：Boiling Water Reactor）であってもよい。

【００３３】

原子炉格納容器１１は、内部に加圧水型原子炉１２と複数（図示は１個）の蒸気発生器１３が格納されている。加圧水型原子炉１２と各蒸気発生器１３は、高温側送給配管１４と低温側送給配管１５を介して連結されており、低温側送給配管１５に一次系冷却水ポンプ１６が設けられている。

【００３４】

加圧器１７は、下部が１個の高温側送給配管１４に連結されており、低温側送給配管１５から延びるスプレイ配管１８がこの加圧器１７の上部に連通し、中途部にスプレイ弁１９が設けられ、先端部にスプレイノズル２０が設けられている。加圧器１７は、上部に加圧器安全弁２１を有する加圧器安全配管２２の一端部が連結されており、加圧器安全配管２２の他端部が大気に開放している。また、加圧器１７は、上部に加圧器逃がし弁２３を有する加圧器逃がし配管２４の一端部が連結されており、加圧器逃がし配管２４の他端部に加圧器逃がしタンク２５が連結されている。

【００３５】

加圧水型原子炉１２は、内部に炉心２６が設けられており、この炉心２６は、複数の燃料集合体（燃料棒）２７により構成されている。また、加圧水型原子炉１２は、炉心２６における燃料集合体２７の間に複数の制御棒２８が配置されている。この各制御棒２８は、制御棒駆動装置２９により上下移動可能となっている。制御棒駆動装置２９は、制御棒２８を炉心２６に対して抜き差しすることで、原子炉出力を制御することができる。

【００３６】

蒸気発生器１３は、内部に逆Ｕ字形状をなす複数の伝熱管からなる伝熱管群３１が設けられている。複数の伝熱管は、各端部が管板に支持され、入室３２と出室３３に連通しており、入室３２に高温側送給配管１４の端部が連結され、出室３３に低温側送給配管１５の端部が連結されている。また、蒸気発生器１３は、図示しないが、伝熱管群３１の上方に給水を蒸気と熱水とに分離する気水分離器と、この分離された蒸気の湿分を除去して乾き蒸気に近い状態とする湿分分離器が設けられている。

【００３７】

また、加圧水型原子炉１２は、化学体積制御系（ＣＶＣＳ）３４が設けられている。低温側送給配管１５は、一次系冷却水循環ライン３５が設けられており、一次系冷却水循環ライン３５に再生熱交換器３６、非再生冷却器３７、脱塩塔３８、体積制御タンク３９、充填ポンプ４０が設けられている。一次系冷却水循環ライン３５は、一次系冷却水補給ライン４１を介して一次系純水タンク４２に連結され、一次系冷却水補給ライン４１に補給水ポンプ４３が設けられている。一次系冷却水補給ライン４１は、ホウ酸水供給ライン４４を介してホウ酸タンク４５が連結され、ホウ酸水供給ライン４４にホウ酸ポンプ４６が設けられている。加圧水型原子炉１２は、化学体積制御系３４により炉心２６におけるホウ素濃度を調整可能である。

【００３８】

原子炉格納容器１１は、内部に原子炉非常用冷却装置４７が設けられている。原子炉格納容器１１は、下部に燃料取替用水ピット４８が設けられており、この燃料取替用水ピット４８から原子炉格納容器１１の外部を通って再び原子炉格納容器１１内に戻り、加圧水型原子炉１２の上方まで延出される冷却水散布ライン４９が設けられている。この冷却水散布ライン４９は、中間部にスプレイポンプ５０と冷却器５１が設けられ、先端部に多数の噴射ノズル５２が設けられている。また、燃料取替用水ピット４８から原子炉格納容器１１の外部を通って再び原子炉格納容器１１内に戻り、加圧水型原子炉１２に連結される

冷却水供給ライン５３が設けられている。この冷却水供給ライン５３は、安全注入ポンプ５４、開閉弁５５が設けられている。

【００３９】

加圧水型原子炉１２は、炉心２６の燃料集合体２７により一次系冷却水として軽水が加熱され、高温の一次系冷却水が加圧器１７により所定の高圧に維持された状態で、高温側送給配管１４を通して蒸気発生器１３に送られる。この蒸気発生器１３は、高温高圧の一次系冷却水と二次系冷却水との間で熱交換を行うことで二次系蒸気を生成し、冷やされた一次系冷却水が加圧水型原子炉１２に戻される。このとき、制御棒駆動装置２９は、炉心２６から制御棒２８を抜き差しすることで、炉心２６内での核分裂を調整する。即ち、燃料集合体２７を構成する原子燃料が核分裂することで中性子を放出し、軽水が放出された高速中性子の運動エネルギを低下させて熱中性子とし、新たな核分裂を起こしやすくすると共に、発生した熱を奪って冷却する。制御棒駆動装置２９は、全ての制御棒２８を炉心２６に挿入することで、加圧水型原子炉１２を停止することができる。

【００４０】

各蒸気発生器１３は、上端部が配管６１ａを介して蒸気タービン６２と連結されており、この配管６１ａに主蒸気隔離弁６３が設けられている。蒸気タービン６２は、高圧タービン６４と低圧タービン６５を有すると共に、発電機（発電装置）６６が接続されている。また、高圧タービン６４と低圧タービン６５は、その間に湿分分離加熱器６７が設けられている。低圧タービン６５は、復水器６８を有しており、この復水器６８は、配管６１ａからバイパス弁６９を有するタービンバイパス配管７０が接続されると共に、冷却水（例えば、海水）を給排する取水管７１及び排水管７２が連結されており、取水管７１に給水ポンプ（海水ポンプ、循環水ポンプ）７３が装着されている。

【００４１】

復水器６８は、配管６１ｂが接続されており、この配管６１ｂに復水ポンプ７４、グランドコンデンサ７５、復水脱塩装置７６、低圧給水加熱器７７、脱気器７８、主給水ポンプ７９、高圧給水加熱器８０、主給水制御弁８１が設けられている。

【００４２】

また、配管６１ａは、主蒸気逃がし弁８２を有する主蒸気逃がし配管８３の一端部と、主蒸気安全弁８４を有する主蒸気安全配管８５の一端部が接続されており、各配管８３，８５の他端部が大気に開放している。一方、配管６１ｂは、主給水制御弁８１と蒸気発生器１３との間に補助給水配管８６の一端部が接続されており、この補助給水配管８６は開閉弁８７が設けられ、他端部に復水タンク８８が接続されている。補助給水配管８６は、並列して２個の分岐補助給水配管８９，９０が設けられ、分岐補助給水配管８９に補助給水ポンプ９１が設けられ、分岐補助給水配管９０に電動補助給水ポンプ９２が設けられている。補助給水ポンプ９１は、蒸気によりタービンが回転することで駆動し、電動補助給水ポンプ９２は、非常用電源により駆動する。

【００４３】

そのため、蒸気発生器１３にて、二次系冷却水が高温高圧の一次系冷却水と熱交換を行って生成された二次系蒸気は、配管６１ａを通して蒸気タービン６２（高圧タービン６４から低圧タービン６５）に送られ、この蒸気により蒸気タービン６２を駆動して発電機６６により発電を行う。このとき、蒸気発生器１３からの蒸気は、高圧タービン６４を駆動した後、湿分分離加熱器６７で蒸気に含まれる湿分が除去されると共に加熱されてから低圧タービン６５を駆動する。そして、蒸気タービン６２を駆動した蒸気は、復水器６８で海水を用いて冷却されて復水となり、配管６１ｂを通って蒸気発生器１３に戻される。

【００４４】

また、原子力発電プラント１０は、加圧水型原子炉１２や蒸気発生器１３などの運転状態を検出するための各種センサが設けられている。加圧水型原子炉１２は、内部の温度を検出する温度センサ１０１と、内部の圧力を検出する圧力センサ１０２が設けられている。蒸気発生器１３は、二次冷却水の水位を検出する水位センサ１０３と、内部の圧力を検出する圧力センサ１０４が設けられている。また、低温側送給配管１５は、一次冷却水の

温度を検出する温度センサ１０５と、圧力を検出する圧力センサ１０６が設けられている。加圧器１７は、一次冷却水の水位を検出する水位センサ１０７と、内部の圧力を検出する圧力センサ１０８が設けられている。配管６１ａは、主蒸気（一次冷却水）の圧力を検出する圧力センサ１０９と、流量を検出する流量センサ１１０が設けられている。

【００４５】

中央制御室２００は、本実施形態の原子力発電プラントの監視制御装置（以下、監視制御装置）２０１が設けられている。監視制御装置２０１は、運転コンソールや大型表示盤などが配置されるプラントの制御設備である。運転コンソールは、運転員による一体的な監視操作を可能とするため、ハードウェアの監視器具や操作器が設置された中央制御盤などから構成されている。大型表示盤は、プラント全体の情報を提供したり、運転員間の情報を共有したりするため、常時表示すべきパラメータや代表警報を表示する。

【００４６】

原子力発電プラントの監視制御装置２０１は、検出装置としての上述した温度センサ１０１，１０５、圧力センサ１０２，１０４，１０６，１０８，１０９、水位センサ１０３，１０７、流量センサ１１０などの検出結果が入力される。また、監視制御装置２０１は、加圧水型原子炉１２や蒸気発生器１３などの状態を変更するためのプラント機器の駆動装置を制御可能となっている。このプラント機器の駆動装置は、例えば、加圧器１７（スプレイ弁１９、加圧器安全弁２１、加圧器逃がし弁２３）、制御棒駆動装置２９、化学体積制御系３４（充填ポンプ４０、補給水ポンプ４３、ホウ酸ポンプ４６）、原子炉非常用冷却装置４７（スプレイポンプ５０、安全注入ポンプ５４、開閉弁５５）、主蒸気隔離弁６３、バイパス弁６９、給水ポンプ７３、復水ポンプ７４、主給水ポンプ７９、主給水制御弁８１、主蒸気逃がし弁８２、主蒸気安全弁８４、開閉弁８７、補助給水ポンプ９１、電動補助給水ポンプ９２などである。

【００４７】

図１は、本実施形態の原子力発電プラントの監視制御装置を表す概略構成図である。

【００４８】

図１に示すように、監視制御装置２０１は、第１監視制御装置２０２と第２監視制御装置２０３とを有している。第１監視制御装置２０２は、第１操作装置２１１と、第１表示装置２１２と、第１制御装置２１３とを有し、プラント機器の検出装置２１４とプラント機器の駆動装置２１５が接続されている。第２監視制御装置２０３は、第２操作装置２２１と、第２表示装置２２２と、第２制御装置２２３とを有し、検出装置２１４と駆動装置２１５が接続されている。検出装置２１４と駆動装置２１５は、加圧水型原子炉１２に接続されている。なお、第１表示装置２１２と第２表示装置２２２は、共用してもよい。

【００４９】

第１制御装置２１３は、第１操作装置２１１からの操作信号が操作指令ラインＬ１により入力されると共に、検出装置２１４が検出したプラントの運転状態が検出信号ラインＬ４により入力される。第１制御装置２１３は、プラントの運転状態をプラント状態検出ラインＬ２により第１操作装置２１１に出力し、更に、第１操作装置２１１が表示ラインＬ３を通して第１表示装置２１２に出力する。そして、第１制御装置２１３は、操作信号とプラントの運転状態に基づいて駆動制御信号を駆動制御信号ラインＬ５，Ｌ６によりプラント機器の駆動装置２１５に出力する。

【００５０】

なお、この第１制御装置２１３は、図示しないが、多重化（例えば、２重化）された多数決判定装置と、多重化（例えば、２重化）された現場機器制御装置とを有している。この多数決判定装置は、多数決制御ロジック（例えば、２／４制御ロジック）を実行する制御装置である。具体的に、各多数決判定装置は、検出装置２１４から予め設定された所定数以上の異常値が検出されると、異常検出信号を現場機器制御装置に出力する。各多数決判定装置は、それぞれ独立して動作する。

【００５１】

第２制御装置２２３は、第１操作装置２２１からの操作信号が操作指令ラインＬ１１に

より入力されると共に、検出装置２１４が検出したプラントの運転状態が検出信号ラインＬ１４により入力される。第２制御装置２２３は、プラントの運転状態をプラント状態検出ラインＬ１２により第２操作装置２２１に出力し、更に、第２操作装置２２１が表示ラインＬ１３を通して第２表示装置２２２に出力する。そして、第２制御装置２２３は、操作信号とプラントの運転状態に基づいて駆動制御信号を駆動制御信号ラインＬ１５，Ｌ６によりプラント機器の駆動装置２１５に出力する。

【００５２】

第２制御装置２２３は、第１制御装置２１３に対して電気的に独立して設けられている。そして、監視制御装置２０１は、第１制御装置２１３と第２制御装置２２３との間に切替装置２２４が設けられている。切替装置２２４は、第１制御装置２１３からの駆動制御信号よりも第２制御装置２２３からの駆動制御信号を優先的にプラント機器の駆動装置２１５に出力するものである。

【００５３】

即ち、第２制御装置２２３は、入力される原子力発電プラント１０（加圧水型原子炉１２）の運転状態に基づいて原子力発電プラント１０の異常発生を検出したときに、プラント機器の駆動装置２１５に対して駆動制御信号を出力するものである。具体的に、切替装置２２４は、第２制御装置２２３からの駆動制御信号の入力がないときに、第１制御装置２１３からの駆動制御信号を駆動制御信号ラインＬ６によりプラント機器の駆動装置２１５に出力し、第２制御装置２２３からの駆動制御信号の入力があるときに、第１制御装置２１３からの駆動制御信号を遮断し、第２制御装置２２３からの駆動制御信号をプラント機器の駆動装置２１５に出力する。切替装置２２４は、例えば、ＯＲ回路である。

【００５４】

第１監視制御装置２０２は、第１操作装置２１１と第１表示装置２１２と第１制御装置２１３と検出装置２１４と駆動装置２１５とがデジタル回線により接続され、デジタル信号による通信が実行される。一方、第２監視制御装置２０３は、第２操作装置２２１と第２表示装置２２２と第２制御装置２２３と検出装置２１４と駆動装置２１５とがアナログ回線により接続され、アナログ信号による通信が実行される。この場合、切替装置２２４は、デジタル信号とアナログ信号の変換器を有している。また、検出装置２１４及び駆動装置２１５と加圧水型原子炉１２とは、デジタル回線であるが、アナログ回線としてもよい。

【００５５】

そして、第１監視制御装置２０２は、第１操作装置２１１と第１表示装置２１２と第１制御装置２１３と検出装置２１４と駆動装置２１５とが有線ネットワークまたは無線ネットワークにより接続され、第２監視制御装置２０３は、第２操作装置２２１と第２表示装置２２２と第２制御装置２２３と検出装置２１４と駆動装置２１５とが有線ネットワーク（ハードワイヤード）により接続される。

【００５６】

また、第２制御装置２２３は、第１制御装置２１３に対するサイバー攻撃により影響を受けない回路を有している。サイバー攻撃により影響を受けない回路とは、書き換え不能なマイクロプロセッサであって、書き換え不能なマイクロプロセッサとして、例えば、ＦＰＧＡ（field-programmable gate array）、ＡＳＩＣ（application specific integrated circuit）などである。また、サイバー攻撃により影響を受けない回路としては、ソリッドステート回路（ソリッドステートリレー／可動接点部分がない回路／無接点リレー）、回路が焼き付けられた半導体、リレー回路などがある。

【００５７】

第２監視制御装置２０３（第２制御装置２２３）は、第１制御装置２０２（第１制御装置２１３）よりもプラント機器を駆動する機能が制限されている。例えば、第２監視制御装置２０３（第２制御装置２２３）は、原子力発電プラント１０（加圧水型原子炉１２）の起動操作、運転操作、停止操作を行うことができるが、第２監視制御装置２０３（第２制御装置２２３）は、原子力発電プラント１０（加圧水型原子炉１２）の停止操作だけを

行うことができる。そのため、第２監視制御装置２０３は、制御棒駆動装置２９、化学体積制御系３４（ホウ酸ポンプ４６）、原子炉非常用冷却装置４７（スプレイポンプ５０、安全注入ポンプ５４、開閉弁５５）、主蒸気逃がし弁８２、主蒸気安全弁８４などの操作だけを行うことができる。

【００５８】

本実施形態の監視制御装置２０１は、第１監視制御装置２０２から独立し、且つ、多様なバックアップシステムとして第２監視制御装置２０３を適用することで、サイバーセキュリティ対策設備を構築するものである。第２監視制御装置２０３は、サイバー攻撃に対して悪影響を受けないものであり、第１監視制御装置２０２から独立し、且つ、多様な対策設備が設けられている。そして、この対策設備は、サイバー攻撃による悪意の操作で発生しうる外乱に対し、リアルタイムに検知して緩和することができる機能を有している。即ち、原子力発電プラント１０に設けられた各プラント機器の駆動状態を監視し、駆動状態が予め設定された閾値よりも上回った（悪化して）場合に、緩和機能を自動的に作動させる。この緩和機能とは、駆動装置２１４が危険側に作動しないように、つまり、安全側に作動するように制御する機能である。また、第２監視制御装置２０３は、原子力発電プラント１０の運転状態を表示する機能を有し、現在の運転状態に応じて原子力発電プラント１０の各プラント機器を手動操作する機能を有する。

【００５９】

これらの必要機能は、制御対象の振る舞いなどの解析／評価結果から選定するもので、ＩＴ技術ではなく、原子力発電プラント１０の各種プラント機器の制御対象に対する制御保護技術に基づいて機能設計される。加えて、有効と考えられる機能を全て導入した場合、設備規模が増大することから、制御対象の振る舞い解析を実施することで、設備合理化を図る。そして、第２監視制御装置２０３は、機能要求が削減されている。緩和機能が要求されるまでの時間が十分確保できる場合や、他機能で代替が可能と判断できる場合は、機能要求から除外する。そして、選定された機能に対し、既存設備で代替可能な場合は、既存設備を用いることで、設備対応の合理化を図る。

【００６０】

ここで、本実施形態の原子力発電プラントの監視制御装置２０１の作用を説明する。図２は、本実施形態の原子力発電プラントの監視制御装置の動作を表すフローチャートである。

【００６１】

図１及び図２に示すように、原子力発電プラント１０の正常時、第２制御装置２２３は、プラント機器の駆動装置２１５に対して駆動制御信号を出力していないことから、切替装置２２４は、第２制御装置２１３からの駆動制御信号を駆動制御信号ラインＬ６によりプラント機器の駆動装置２１５に出力し、加圧水型原子炉１２を含む原子力発電プラント１０の起動操作、運転操作、停止操作を行うと共に、運転状態を監視している。このとき、オペレータは、第１表示装置２１２に表示された原子力発電プラント１０の運転状態を監視しながら、手動により第１操作装置２１１を操作することもできる。

【００６２】

ステップＳ１１にて、原子力発電プラント１０の運転制御に外乱が発生し、ステップＳ１２にて、加圧水型原子炉１２の機能が悪化したとき、ステップＳ１３にて、第２制御装置２２３は、異常が発生したかどうかを判定する。ここで、サイバー攻撃でないと判定（Ｎｏ）したとき、第１制御装置２１３がプラント機器の駆動装置２１５を制御することで外乱が取り除かれ、加圧水型原子炉１２の機能悪化が改善されるため、何もしないでこのルーチンを抜ける。

【００６３】

一方、サイバー攻撃であると判定（Ｙｅｓ）したときは、第１制御装置２１３がプラント機器の駆動装置２１５を制御しても外乱が取り除かれず、加圧水型原子炉１２の機能悪化が継続する。このとき、ステップＳ１４にて、第２制御装置２２３は、緩和機能を作動させる。即ち、第２制御装置２２３は、原子力発電プラント１０の異常を検出することで

駆動制御信号を出力する。切替装置２２４は、第２制御装置２２３から駆動制御信号の入力を受け、第１制御装置２１３からの駆動制御信号を遮断し、第２制御装置２２３からの駆動制御信号をプラント機器の駆動装置２１５に出力する。このとき、オペレータは、第２表示装置２１２に表示された原子力発電プラント１０の運転状態を監視しながら、手動により第２操作装置２２１を操作することもできる。

【００６４】

この場合、例えば、炉心２６の温度が上昇しているにも拘らず、冷却水量が予め設定された所定量以下であれば、安全注入ポンプ５４（図３参照）を作動して冷却水量を増加させる処理を実行する。また、炉心２６の温度が上昇し、冷却水量を増加させているにも拘らず、炉心２６の温度が低下しないときは、制御棒駆動装置２９を作動して制御棒を炉心に挿入する処理を実行する。また、常用電源が喪失した場合には、非常用電源を使用する。このような処理は、全て安全側に向かうような処理を実行する。

【００６５】

そして、ステップＳ１５にて、第２制御装置２２３は、原子力発電プラント１０の異常が収束したかどうかを判定する。ここで、異常が収束していないと判定（Ｎｏ）したときは、ステップＳ１４の処理を継続する。一方、異常が収束したと判定（ＹＥＳ）したときは、ステップＳ１６にて、原子力発電プラント１０が安定化したことを確認し、高温停止を維持するか、または、低温停止に移行する操作を実行する。

【００６６】

このように本実施形態のプラントの監視制御装置にあっては、原子力発電プラント１０の運転状態が入力されると共にプラント機器に対して駆動制御信号を出力する第１制御装置２１３と、第１制御装置２１３に対して電気的に独立して設けられて原子力発電プラント１０の運転状態が入力されると共にプラント機器に対して駆動制御信号を出力する第２制御装置２２３と、第１制御装置２１３からの駆動制御信号よりも第２制御装置２２３からの駆動制御信号を優先的にプラント機器に出力する切替装置２２４とを備えている。

【００６７】

従って、第２制御装置２２３が第１制御装置２１３に対して電気的に独立して設けられており、切替装置２２４により第２制御装置２２３からの駆動制御信号が第１制御装置２１３からの駆動制御信号よりも優先的にプラント機器の駆動装置２１５に出力されることから、例えば、サイバー攻撃により第１制御装置２１３によるプラント制御の健全性が損なわれても、第１制御装置２１３に代わって第２制御装置２２３が優先的にプラント機器の駆動装置２１５を制御することとなり、原子力発電プラント１０の安全性を維持することができる。

【００６８】

即ち、従来のサイバー攻撃に対する対策は、ＩＴ技術をベースとした制御システムであって、プラントにおける異常の発生を防止するものであるが、本実施形態は、制御対象となるプラントの制御保護設計技術をベースとし、プラントの異常を検知し、プラント機器への悪影響をリアルタイムに緩和するものである。つまり、本実施形態の対策設備は、システムの基本となる第１監視制御装置２０２とは独立し、且つ、多様な第２監視制御装置２０３を構築し、プラントの異常を制御保護の観点から直接緩和するものであり、サイバー攻撃への耐性が高い。

【００６９】

本実施形態のプラントの監視制御装置では、第２制御装置２２３は、入力される原子力発電プラント１０の運転状態に基づいて原子力発電プラント１０の異常発生を検出したときに、プラント機器の駆動装置２１５に対して駆動制御信号を出力する。従って、原子力発電プラント１０の正常時は、第１制御装置２１３が原子力発電プラント１０の運転状態に基づいた駆動制御信号をプラント機器の駆動装置２１５に出力し、原子力発電プラント１０の異常発生は、第２制御装置２２３が原子力発電プラント１０の運転状態に基づいた駆動制御信号をプラント機器の駆動装置２１５に出力することで、第１制御装置２１３がサイバー攻撃により乗っ取られても、第２制御装置２２３がプラント機器の駆動装置２１

５を安全に制御することができる。
【００７０】
本実施形態のプラントの監視制御装置では、切替装置２２４は、第２制御装置２２３からの駆動制御信号の入力がないときに第１制御装置２１３からの駆動制御信号をプラント機器の駆動装置２１５に出力し、第２制御装置２２３からの駆動制御信号の入力があるときに第２制御装置２２３からの駆動制御信号をプラント機器の駆動装置２１５に出力する。従って、原子力発電プラント１０の正常時は、切替装置２２４に第２制御装置２２３からの駆動制御信号の入力がないことから、第１制御装置２１３が原子力発電プラント１０の運転状態に基づいてプラント機器の駆動装置２１５を制御し、第１制御装置２１３がサイバー攻撃により原子力発電プラント１０を不安定にさせる駆動制御信号を出力したとき、第２制御装置２２３が原子力発電プラント１０を安定させる駆動制御信号を出力し、切替装置２２４は、第２制御装置２２３の駆動制御信号をプラント機器の駆動装置２１５に出力することで、第２制御装置２２３がプラント機器の駆動装置２１５を安全に制御することができる。
【００７１】
本実施形態のプラントの監視制御装置では、切替装置２２４は、第２制御装置２２３からの駆動制御信号の入力があるときに、第１制御装置２１３からの駆動制御信号を遮断して第２制御装置２２３からの駆動制御信号をプラント機器の駆動装置２１５に出力するＯＲ回路である。従って、第１制御装置２１３がサイバー攻撃により原子力発電プラント１０を不安定にさせる駆動制御信号を出力したとき、第２制御装置２２３が原子力発電プラント１０を安定させる駆動制御信号を出力し、切替装置２２４としてのＯＲ回路は、第１制御装置２１３からの駆動制御信号を遮断し、第２制御装置２２３からの駆動制御信号をプラント機器の駆動装置２１５に出力するため、第２制御装置２２３の駆動制御信号によりプラント機器の駆動装置２１５を安全に制御することができる。
【００７２】
本実施形態のプラントの監視制御装置では、第１制御装置２１３は、駆動制御信号としてのデジタル信号を出力し、第２制御装置２２３は、駆動制御信号としてのアナログ信号を出力する。従って、第２制御装置２２３は、第１制御装置２１３が取り扱うデジタル信号と異なる形式のアナログ信号を用いることで、サイバー攻撃により第１制御装置２１３にコンピュータウイルスが侵入しても、第２制御装置２２３まで感染することが抑制され、第２制御装置２２３によりプラント機器の駆動装置２１５を安全に制御することができる。
【００７３】
本実施形態のプラントの監視制御装置では、第２制御装置２２３は、書き換え不能なマイクロプロセッサを有している。従って、サイバー攻撃により第１制御装置２１３にコンピュータウイルスが侵入しても、コンピュータウイルスにより第２制御装置２２３のマイクロプロセッサが書き換えられることがなく、第２制御装置２２３によりプラント機器の駆動装置２１５を安全に制御することができる。
【００７４】
本実施形態のプラントの監視制御装置では、第２制御装置２２３は、原子力発電プラント１０の運転状態を検出する検出装置２１４とプラント機器の駆動装置２１５とがハードワイヤードにより接続されている。従って、第２制御装置２２３が無線回線や有線回線などを用いたネットワークからのサイバー攻撃を受けることがなく、第２制御装置２２３によりプラント機器の駆動装置２１５を安全に制御することができる。
【００７５】
本実施形態のプラントの監視制御装置では、第２制御装置２２３は、第１制御装置２１３よりもプラント機器を駆動する駆動装置２１５の機能が制限されている。従って、第２制御装置２２３の機能は、第１制御装置２１３の機能よりも縮小されることで、第２制御装置２２３の設置による製造コストの増加を抑制することができる。
【００７６】

本実施形態のプラントの監視制御装置では、第１制御装置２１３は、原子力発電プラント１０の起動操作、運転操作、停止操作を行うものであり、第２制御装置２２３は、原子力発電プラント１０の停止操作だけを行うものである。従って、第１制御装置２１３が原子力発電プラント１０の起動操作、運転操作、停止操作を行うことから、原子力発電プラント１０の正常時にプラント機器の駆動装置２１５を正常に運転することができ、第２制御装置２２３が原子力発電プラント１０の停止操作だけを行うことから、第１制御装置２１３による原子力発電プラント１０の制御が異常であるとき、第２制御装置２２３が原子力発電プラント１０を安全に停止させることができる。

【００７７】

本実施形態のプラントの監視制御装置では、第２制御装置２２３は、原子力発電プラント１０の運転状態を表示する第２表示装置２２２と、第２制御装置２２３に操作信号を入力する第２操作装置２２１を接続している。従って、原子力発電プラント１０の異常発生時に、第２表示装置２２２に原子力発電プラント１０の運転状態が表示されることから、オペレータは、第２表示装置２２２を見ながら第２操作装置２２１を用いて第２制御装置２２３に操作信号を出力することができ、プラント１０を安全に運転することができる。

【００７８】

なお、上述した実施形態では、本発明のプラントの監視制御装置を原子力発電プラント１０に適用して説明したが、例えば、火力や水力などの発電プラント、化学プラント、その他の機械、電気、水道などのプラントに適用してもよい。

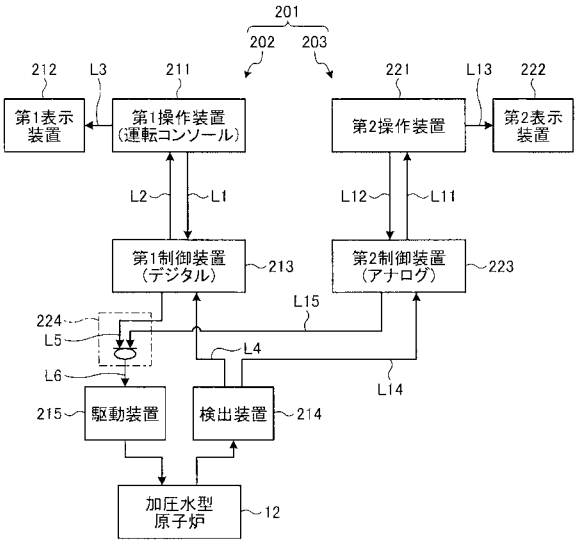
【符号の説明】

【００７９】

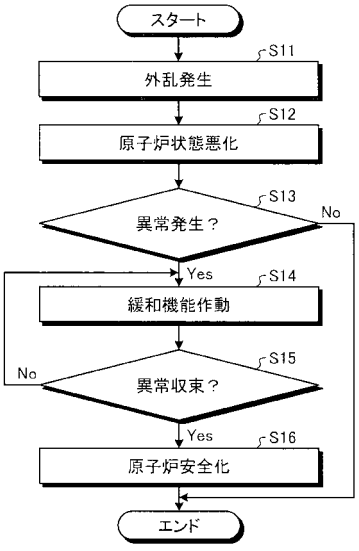
１０　原子力発電プラント
１１　原子炉格納容器
１２　加圧水型原子炉
１３　蒸気発生器
１４　高温側送給配管
１５　低温側送給配管
１７　加圧器
２３　加圧器逃がし弁
２６　炉心
２７　燃料集合体
２８　制御棒
２９　制御棒駆動装置
３１　伝熱管群
３４　化学体積制御系
４７　原子炉非常用冷却装置
６１ａ，６１ｂ　配管
６２　蒸気タービン
６６　発電機
６８　復水器
１０１，１０５　温度センサ
１０２，１０４，１０６，１０８，１０９　圧力センサ
１０３，１０７　水位センサ
１１０　流量センサ
２００　中央制御室
２０１　監視制御装置
２０２　第１監視制御装置
２０３　第２監視制御装置
２１１　第１操作装置
２１２　第１表示装置

２１３　第１制御装置
２１４　検出装置
２１５　駆動装置
２２１　第２操作装置
２２２　第２表示装置
２２３　第２制御装置
２２４　切替装置（ＯＲ回路）

【図１】



【図２】



【図３】