(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)公開番号
特開2023-40088
(P2023-40088A)
(43)公開日　令和5年3月22日(2023.3.22)

(51)国際特許分類　F I
G21D 3/04 (2006.01)　G21D 3/04 A

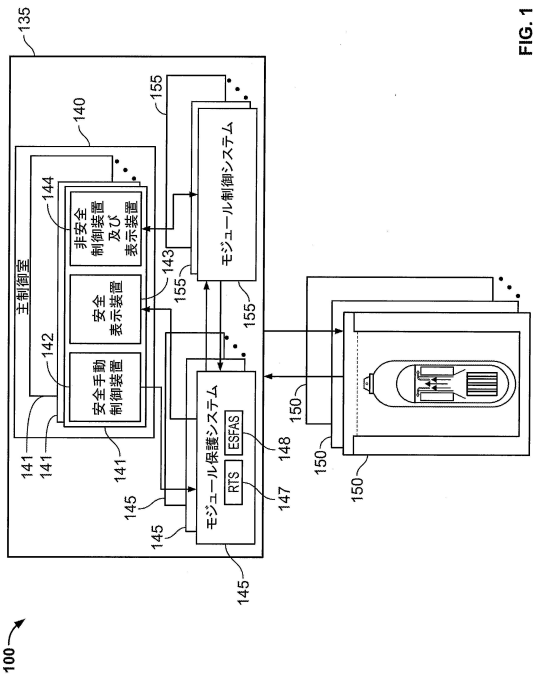
審査請求　有　請求項の数　20　ＯＬ　外国語出願　（全47頁）

(21)出願番号　特願2022-208089(P2022-208089)
(22)出願日　令和4年12月26日(2022.12.26)
(62)分割の表示　特願2021-99632(P2021-99632)の分割
原出願日　平成26年12月23日(2014.12.23)
(31)優先権主張番号　61/922,625
(32)優先日　平成25年12月31日(2013.12.31)
(33)優先権主張国・地域又は機関　米国(US)
(31)優先権主張番号　14/198,891
(32)優先日　平成26年3月6日(2014.3.6)
(33)優先権主張国・地域又は機関　米国(US)

(71)出願人　511117093
ニュースケール パワー エルエルシー
アメリカ合衆国 ９７３３０ オレゴン州 コーバリス ノースイースト サークル ブールバード １１００ スイート ２００
(71)出願人　516197425
ロック クリーク イノベーションズ エルエルシー
アメリカ合衆国 カンザス州 ６６８７１ ウェイバリー リーパー ロード ２５３９
(74)代理人　100083806
弁理士　三好 秀和
(74)代理人　100111235
弁理士　原 裕子
(74)代理人　100195257
最終頁に続く

(54)【発明の名称】　原子炉保護システム及び方法

(57)【要約】　（修正有）
【課題】複数の機能的に独立したモジュールの各々は、複数の機能的に独立したモジュールのうちのあらゆる他のモジュールに対する単一の故障伝搬に対する保護を提供すること。
【解決手段】原子炉保護システムは、複数の機能的に独立したモジュールであって、モジュールの各々が、原子炉安全システムから複数の入力を受信し、少なくとも部分的に複数の入力に基づいて安全動作を論理的に決定するように構成された、複数の機能的に独立したモジュールと、複数の機能的に独立したモジュールに通信可能に接続され、少なくとも部分的に複数の入力に基づいて安全動作の決定を受信する１つ又は複数の原子炉安全アクチュエータとを備える。
【選択図】図１



【特許請求の範囲】
【請求項１】
原子炉保護システムであって、
複数の機能的に独立したモジュールであって、前記モジュールの各々は、原子炉安全システムから複数の入力を受信し、少なくとも部分的に前記複数の入力に基づいて安全動作を論理的に決定するように構成される、複数の機能的に独立したモジュールと、
前記複数の機能的に独立したモジュールに通信可能に接続され、少なくとも部分的に前記複数の入力に基づく前記安全動作決定を受信する、１つ又は複数の原子炉安全アクチュエータと
を備える、原子炉保護システム。
【請求項２】
請求項１に記載の原子炉保護システムであって、
前記複数の機能的に独立したモジュールの各々は、前記複数の機能的に独立したモジュールの他のいずれかのモジュールに対する単一の故障伝搬に対する保護を提供する、原子炉保護システム。
【請求項３】
請求項１に記載の原子炉保護システムであって、
前記原子炉安全システムは、工学的安全施設作動システム（ＥＳＦＡＳ）を備え、
前記複数の機能的に独立したモジュールは、複数のＥＳＦＡＳ入力を受信し、少なくとも部分的に前記ＥＳＦＡＳ入力に基づいてＥＳＦＡＳコンポーネントの作動を論理的に決定する、原子炉保護システム。
【請求項４】
請求項３に記載の原子炉保護システムであって、
前記複数の機能的に独立したモジュールは、冗長ＥＳＦＡＳ投票区分を提供する、原子炉保護システム。
【請求項５】
請求項１に記載の原子炉保護システムであって、
前記原子炉安全システムは、原子炉トリップシステム（ＲＴＳ）を備え、
前記複数の機能的に独立したモジュールは、複数のＲＴＳ入力を受信し、少なくとも部分的に前記ＲＴＳ入力に基づいてＲＴＳコンポーネントの作動を論理的に決定する、原子炉保護システム。
【請求項６】
請求項５に記載の原子炉保護システムであって、
前記複数の機能的に独立したモジュールは、冗長ＲＴＳ投票区分を提供する、原子炉保護システム。
【請求項７】
請求項１に記載の原子炉保護システムであって、
前記複数の機能的に独立したモジュールの各々は、前記複数の機能的に独立したモジュールのうちの他のいずれかへの単一のハードウェア故障伝搬に対する保護を提供する、原子炉保護システム。
【請求項８】
請求項１に記載の原子炉保護システムであって、
前記複数の機能的に独立したモジュールの各々は、前記複数の機能的に独立したモジュールのうちの他のいずれかへの単一のソフトウェア故障伝搬に対する保護を提供する、原子炉保護システム。
【請求項９】
請求項１に記載の原子炉保護システムであって、
前記複数の機能的に独立したモジュールの各々は、前記複数の機能的に独立したモジュールのうちの他のいずれかへの単一のソフトウェア生成論理故障伝搬に対する保護を提供する、原子炉保護システム。

【請求項１０】
請求項１に記載の原子炉保護システムであって、
前記複数の機能的に独立したモジュールは、原子炉トリップ検知及び決定の単一の経路について３重冗長化を提供する、原子炉保護システム。
【請求項１１】
請求項１に記載の原子炉保護システムであって、
前記複数の機能的に独立したモジュールは、原子炉トリップコンポーネント毎に複数の独立したトリップ投票モジュールを備える、原子炉保護システム。
【請求項１２】
請求項１に記載の原子炉保護システムであって、
前記複数の機能的に独立したモジュールは、特定のトリップコンポーネントに専用の前記複数のモジュールのうちの他の全てのモジュールから切り離して前記原子炉トリップを論理的に決定する、原子炉保護システム。
【請求項１３】
請求項１に記載の原子炉保護システムであって、
前記複数の機能的に独立したモジュールは、ＥＳＦコンポーネント毎に複数の独立したＥＳＦＡＳ作動投票モジュールを備える、原子炉保護システム。
【請求項１４】
請求項１に記載の原子炉保護システムであって、
前記複数の機能的に独立したモジュールは、特定のＥＳＦコンポーネントに専用の前記複数のモジュールのうちの他の全てから切り離して前記ＥＳＦＡＳ作動を論理的に決定する、原子炉保護システム。
【請求項１５】
請求項１に記載の原子炉保護システムであって、
前記複数の機能的に独立したモジュールは、複数の安全機能モジュールを備える、原子炉保護システム。
【請求項１６】
請求項１に記載の原子炉保護システムであって、
前記複数の機能的に独立したモジュールは、複数の通信モジュールを備える、原子炉保護システム。
【請求項１７】
請求項１に記載の原子炉保護システムであって、
前記複数の機能的に独立したモジュールは、複数の機器インタフェースモジュールを備える、原子炉保護システム。
【請求項１８】
請求項１に記載の原子炉保護システムであって、
前記複数の機能的に独立したモジュールは、単一階層投票スキームにおいて前記原子炉トリップを論理的に決定する、原子炉保護システム。
【請求項１９】
請求項１に記載の原子炉保護システムであって、
前記複数の機能的に独立したモジュールは、複数階層投票スキームにおいて前記原子炉トリップを論理的に決定する、原子炉保護システム。
【請求項２０】
請求項１９に記載の原子炉保護システムであって、
前記複数階層投票スキームは、２階層投票スキームを備える、原子炉保護システム。
【請求項２１】
請求項２０に記載の原子炉保護システムであって、
前記２階層投票スキームの第１の階層は、多数決投票スキームを備える、原子炉保護システム。
【請求項２２】

請求項２１に記載の原子炉保護システムであって、
前記多数決投票スキームは、３分の２投票スキームを備える、原子炉保護システム。
【請求項２３】
請求項２０に記載の原子炉保護システムであって、
前記２階層投票スキームの第２の階層は、非多数決投票スキームを備える、原子炉保護システム。
【請求項２４】
請求項２３に記載の原子炉保護システムであって、
前記第２の階層は、４分の２投票スキームを備える、原子炉保護システム。
【請求項２５】
原子炉トリップを決定するための方法であって、
工学的安全施設作動システム（ＥＳＦＡＳ）又は原子炉トリップシステム（ＲＴＳ）のうちの一方から、原子炉保護システムの複数の機能的に独立したモジュールにおいて複数の入力を受信することと、
前記複数の機能的に独立したモジュールによって、少なくとも部分的に前記複数の入力に基づいてＥＳＦＡＳ安全動作又は原子炉トリップの決定のうちの一方を論理的に決定することと、
前記論理的な決定に基づいて、前記複数の機能的に独立したモジュールに通信可能に接続されたＥＳＦＡＳコンポーネントアクチュエータ又は原子炉トリップ遮断器のうちの一方を作動させることと
を備える、方法。
【請求項２６】
請求項２５に記載の方法であって、
前記複数の機能的に独立したモジュールのうちの１つによって、前記複数の機能的に独立したモジュールのうちの他のいずれかへの単一の故障伝搬を制限することを更に備える、方法。
【請求項２７】
請求項２６に記載の方法であって、
前記単一の故障は、単一のハードウェア故障、単一のソフトウェア故障、又は単一のソフトウェア生成論理故障のうちの少なくとも１つを含む、方法。
【請求項２８】
請求項２５に記載の方法であって、
前記複数の機能的に独立したモジュールによって、少なくとも部分的に前記入力に基づいてＥＳＦＡＳ安全動作又は原子炉トリップの決定のうちの一方を論理的に決定することは、前記複数の機能的に独立したモジュールによって、３重冗長化信号経路を通して前記ＥＳＦＡＳ安全動作又は前記原子炉トリップの決定を論理的に決定することを備える、方法。
【請求項２９】
請求項２５に記載の方法であって、
前記複数の機能的に独立したモジュールは、冗長ＲＴＳ投票区分又は冗長ＥＳＦＡＳ投票区分のうちの少なくとも一方を提供する、方法。
【請求項３０】
請求項２５に記載の方法であって、
前記複数の機能的に独立したモジュールによって、少なくとも部分的に前記入力に基づいてＥＳＦＡＳ安全動作又は原子炉トリップの決定のうちの一方を論理的に決定することは、前記複数の機能的に独立したモジュールによって、原子炉トリップコンポーネント毎の複数の独立したトリップ投票モジュールを通して前記ＥＳＦＡＳ安全動作又は前記原子炉トリップの決定を論理的に決定することを備える、方法。
【請求項３１】
請求項３０に記載の方法であって、

前記複数の機能的に独立したモジュールによって、少なくとも部分的に前記入力に基づいてＥＳＦＡＳ安全動作又は原子炉トリップの決定のうちの一方を論理的に決定することは、前記複数の機能的に独立したモジュールのうちの特定のモジュールによって、前記複数のモジュールのうちの全ての他のモジュールから切り離して前記ＥＳＦＡＳ安全動作又は前記原子炉トリップの決定を論理的に決定することを備える、方法。

【請求項３２】

請求項２５に記載の方法であって、

前記複数の機能的に独立したモジュールは、ＥＳＦコンポーネント毎に複数の独立したＥＳＦＡＳ作動投票モジュールを備え、

前記方法は、更に、

前記複数の機能的に独立したモジュールのうちの特定のモジュールによって、特定のＥＳＦコンポーネントに専用の前記複数のモジュールのうちの全ての他のモジュールから切り離して前記ＥＳＦＡＳ作動を論理的に決定することを備える、方法。

【請求項３３】

請求項２５に記載の方法であって、

前記複数の機能的に独立したモジュールは、複数の安全機能モジュールと、複数の通信モジュールと、複数の機器インタフェースモジュールとを備える、方法。

【請求項３４】

請求項２５に記載の方法であって、

前記複数の機能的に独立したモジュールによって、少なくとも部分的に前記入力に基づいてＥＳＦＡＳ安全動作又は原子炉トリップの決定のうちの一方を論理的に決定することは、前記複数の機能的に独立したモジュールによって、単一階層投票スキームにおいて前記ＥＳＦＡＳ安全動作又は前記原子炉トリップの決定を論理的に決定することを備える、方法。

【請求項３５】

請求項２５に記載の方法であって、

前記複数の機能的に独立したモジュールによって、少なくとも部分的に前記入力に基づいてＥＳＦＡＳ安全動作又は原子炉トリップの決定のうちの一方を論理的に決定することは、前記複数の機能的に独立したモジュールによって、複数階層投票スキームにおいて前記ＥＳＦＡＳ安全動作又は前記原子炉トリップの決定を論理的に決定することを備える、方法。

【請求項３６】

請求項３５に記載の方法であって、

前記複数階層投票スキームは、２階層投票スキームを備える、方法。

【請求項３７】

請求項３６に記載の方法であって、

前記２階層投票スキームの第１の階層は、多数決投票スキームを備える、方法。

【請求項３８】

請求項３７に記載の方法であって、

前記多数決投票スキームは、３分の２投票スキームを備える、方法。

【請求項３９】

請求項３６に記載の方法であって、

前記２階層投票スキームの第２の階層は、非多数決投票スキームを備える、方法。

【請求項４０】

請求項３９に記載の方法であって、

前記第２の階層は、４分の２投票スキームを備える、方法。

【請求項４１】

原子炉保護装置であって、

原子炉安全システムから複数の入力を受信し、少なくとも部分的に前記複数の入力に基づいて安全動作を論理的に決定するための手段と、

少なくとも部分的に前記複数の入力に基づいて前記安全動作の決定を受信するための手段と
を備える、原子炉保護装置。
【請求項４２】
請求項４１に記載の原子炉保護装置であって、
前記安全動作の決定を受信するための前記手段は、前記原子炉安全システムから前記複数の入力を受信し、前記安全動作を論理的に決定するための前記手段に通信可能に接続されている、原子炉保護装置。
【請求項４３】
請求項４１に記載の原子炉保護装置であって、
前記原子炉安全システムから前記複数の入力を受信し、前記安全動作を論理的に決定するための前記手段は、前記装置内の単一の故障伝搬に対する保護を提供する、原子炉保護装置。
【請求項４４】
請求項４１に記載の原子炉保護装置であって、
前記原子炉安全システムは、工学的安全施設作動システム（ＥＳＦＡＳ）を備え、
前記原子炉安全システムから前記複数の入力を受信し、前記安全動作を論理的に決定するための前記手段は、複数のＥＳＦＡＳ入力を受信し、少なくとも部分的に前記ＥＳＦＡＳ入力に基づいてＥＳＦＡＳコンポーネントの作動を論理的に決定する、原子炉保護装置。
【請求項４５】
請求項４４に記載の原子炉保護装置であって、
前記原子炉安全システムから前記複数の入力を受信し、前記安全動作を論理的に決定するための前記手段は、冗長ＥＳＦＡＳ投票区分を提供する、原子炉保護装置。
【請求項４６】
請求項４１に記載の原子炉保護装置であって、
前記原子炉安全システムは、原子炉トリップシステム（ＲＴＳ）を備え、
前記原子炉安全システムから前記複数の入力を受信し、前記安全動作を論理的に決定するための前記手段は、複数のＲＴＳ入力を受信し、少なくとも部分的に前記ＲＴＳ入力に基づいてＲＴＳコンポーネントの作動を論理的に決定する、原子炉保護装置。
【請求項４７】
請求項４６に記載の原子炉保護装置であって、
前記原子炉安全システムから前記複数の入力を受信し、前記安全動作を論理的に決定するための前記手段は、冗長ＲＴＳ投票区分を備える、原子炉保護装置。
【請求項４８】
請求項４１に記載の原子炉保護装置であって、
前記原子炉安全システムから前記複数の入力を受信し、前記安全動作を論理的に決定するための前記手段は、前記装置内の単一のハードウェア故障伝搬に対する保護を提供する、原子炉保護装置。
【請求項４９】
請求項４１に記載の原子炉保護装置であって、
前記原子炉安全システムから前記複数の入力を受信し、前記安全動作を論理的に決定するための前記手段は、前記装置内の単一のソフトウェア故障伝搬に対する保護を提供する、原子炉保護装置。
【請求項５０】
請求項４１に記載の原子炉保護装置であって、
前記原子炉安全システムから前記複数の入力を受信し、前記安全動作を論理的に決定するための前記手段は、前記装置内の単一のソフトウェア生成論理故障伝搬に対する保護を提供する、原子炉保護装置。
【請求項５１】

請求項４１に記載の原子炉保護装置であって、
前記原子炉安全システムから前記複数の入力を受信し、前記安全動作を論理的に決定するための前記手段は、原子炉トリップ検知及び決定の３重冗長信号経路を備える、原子炉保護装置。
【請求項５２】
請求項４１に記載の原子炉保護装置であって、
前記原子炉安全システムから前記複数の入力を受信し、前記安全動作を論理的に決定するための前記手段は、原子炉トリップコンポーネント毎に複数の独立したトリップ投票モジュールを備える、原子炉保護装置。
【請求項５３】
請求項４１に記載の原子炉保護装置であって、
前記原子炉安全システムから前記複数の入力を受信し、前記安全動作を論理的に決定するための前記手段は、特定の原子炉トリップコンポーネントについて原子炉トリップを独立して決定する、原子炉保護装置。
【請求項５４】
請求項４１に記載の原子炉保護装置であって、
前記原子炉安全システムから前記複数の入力を受信し、前記安全動作を論理的に決定するための前記手段は、ＥＳＦコンポーネント毎に複数の独立したＥＳＦＡＳ作動投票モジュールを備える、原子炉保護装置。
【請求項５５】
請求項４１に記載の原子炉保護装置であって、
前記原子炉安全システムから前記複数の入力を受信し、前記安全動作を論理的に決定するための前記手段は、特定のＥＳＦコンポーネントについてＥＳＦＡＳ作動を独立して決定する、原子炉保護装置。
【請求項５６】
請求項４１に記載の原子炉保護装置であって、
前記原子炉安全システムから前記複数の入力を受信し、前記安全動作を論理的に決定するための前記手段は、複数の安全機能モジュールを備える、原子炉保護装置。
【請求項５７】
請求項４１に記載の原子炉保護装置であって、
前記原子炉安全システムから前記複数の入力を受信し、前記安全動作を論理的に決定するための前記手段は、複数の通信モジュールを備える、原子炉保護装置。
【請求項５８】
請求項４１に記載の原子炉保護装置であって、
前記原子炉安全システムから前記複数の入力を受信し、前記安全動作を論理的に決定するための前記手段は、複数の機器インタフェースモジュールを備える、原子炉保護装置。
【請求項５９】
請求項４１に記載の原子炉保護装置であって、
前記原子炉安全システムから前記複数の入力を受信し、前記安全動作を論理的に決定するための前記手段は、単一階層投票スキームにおいて原子炉トリップを論理的に決定する、原子炉保護装置。
【請求項６０】
請求項４１に記載の原子炉保護装置であって、
前記原子炉安全システムから前記複数の入力を受信し、前記安全動作を論理的に決定するための前記手段は、複数階層投票スキームにおいて原子炉トリップを論理的に決定する、原子炉保護装置。
【請求項６１】
請求項６０に記載の原子炉保護装置であって、
前記複数階層投票スキームは、２階層投票スキームを備える、原子炉保護装置。
【請求項６２】

請求項６１に記載の原子炉保護装置であって、
前記２階層投票スキームの第１の階層は、多数決投票スキームを備える、原子炉保護装置。
【請求項６３】
請求項６２に記載の原子炉保護装置であって、
前記多数決投票スキームは、３分の２投票スキームを備える、原子炉保護装置。
【請求項６４】
請求項６１に記載の原子炉保護装置であって、
前記２階層投票スキームの第２の階層は、非多数決投票スキームを備える、原子炉保護装置。
【請求項６５】
請求項６４に記載の原子炉保護装置であって、
前記第２の階層は、４分の２投票スキームを備える、原子炉保護装置。
【発明の詳細な説明】
【技術分野】
【０００１】
[関連出願に対する相互参照]
本願は、２０１３年１２月３１日に出願された米国仮特許出願第６１／９２２，６２５号及び２０１４年３月６日に出願された米国特許出願第１４／１９８，８９１号に対して優先権を主張し、両出願の全内容が参照によりここに援用される。
[技術的背景]
本開示は、原子炉保護システム及びその関連する方法を述べる。
[背景]
原子炉保護システム、及び一般的に、原子炉計装制御（Ｉ＆Ｃ）システムは、故障状態がもたらす結果を軽減するため、自動始動信号、自動及び手動制御信号、並びに監視表示を提供する。例えば、Ｉ＆Ｃシステムは、定常状態及び過渡的電力運転中に安全でない原子炉運転に対する保護を提供する。正常運転中、Ｉ＆Ｃシステムは、種々のパラメータを測定し、それらの信号を制御システムに送信する。異常運転及び事故状態中に、Ｉ＆Ｃシステムは、信号を、原子炉保護システムに、幾つかの場合には原子炉保護システムの原子炉トリップシステム（ＲＴＳ）及び工学的安全施設作動システム（ＥＳＦＡＳ）に送信して、所定の設定点に基づいて保護動作を開始する。
[概要]
本開示に係る全体的な実装形態において、原子炉保護システムは、複数の機能的に独立したモジュールであって、モジュールの各々は、原子炉安全システムから複数の入力を受信し、少なくとも部分的に複数の入力に基づいて安全動作を論理的に決定するように構成された、複数の機能的に独立したモジュールと、少なくとも部分的に複数の入力に基づいた安全動作決定を受信するために、複数の機能的に独立したモジュールに通信可能に接続された１つ又は複数の原子炉安全アクチュエータとを含んでいる。
【０００２】
全体的な実装形態と組合せ可能な第１の局面において、複数の機能的に独立したモジュールの各々は、複数の機能的に独立したモジュールのうちのあらゆる他のモジュールに対する単一の故障伝搬に対する保護を提供する。
【０００３】
前の局面のうちのいずれかと組合せ可能な第２の局面において、原子炉安全システムは、工学的安全施設作動システム（ＥＳＦＡＳ）を含み、複数の機能的に独立したモジュールは、複数のＥＳＦＡＳ入力を受信し、少なくとも部分的にＥＳＦＡＳ入力に基づいてＥＳＦＡＳコンポーネント作動を論理的に決定する。
【０００４】
前の局面のうちのいずれかと組合せ可能な第３の局面において、複数の機能的に独立したモジュールは、冗長ＥＳＦＡＳ投票区分を提供する。

前の局面のうちのいずれかと組合せ可能な第４の局面において、原子炉安全システムは、原子炉トリップシステム（ＲＴＳ）を含み、複数の機能的に独立したモジュールは、複数のＲＴＳ入力を受信し、少なくとも部分的にＲＴＳ入力に基づいてＲＴＳコンポーネント作動を論理的に決定する。

【０００５】

前の局面のうちのいずれかと組合せ可能な第５の局面において、複数の機能的に独立したモジュールは、冗長ＲＴＳ投票区分を提供する。

前の局面のうちのいずれかと組合せ可能な第６の局面において、複数の機能的に独立したモジュールの各々は、複数の機能的に独立したモジュールのうちのいずれかの他のモジュールに対する単一のハードウェア故障伝搬に対する保護を提供する。

【０００６】

前の局面のうちのいずれかと組合せ可能な第７の局面において、複数の機能的に独立したモジュールの各々は、複数の機能的に独立したモジュールのうちのいずれかの他のモジュールに対する単一のソフトウェア故障伝搬に対する保護を提供する。

【０００７】

前の局面のうちのいずれかと組合せ可能な第８の局面において、複数の機能的に独立したモジュールの各々は、複数の機能的に独立したモジュールのうちのいずれかの他のモジュールに対する単一のソフトウェア生成論理故障伝搬に対する保護を提供する。

【０００８】

前の局面のうちのいずれかと組合せ可能な第９の局面において、複数の機能的に独立したモジュールは、原子炉トリップ検知及び決定の単一の経路について３重冗長化を提供する。

【０００９】

前の局面のうちのいずれかと組合せ可能な第１０の局面において、複数の機能的に独立したモジュールは、原子炉トリップコンポーネント毎に複数の独立したトリップ投票モジュールを含む。

【００１０】

前の局面のうちのいずれかと組合せ可能な第１１の局面において、複数の機能的に独立したモジュールは、特定のトリップコンポーネントに専用の複数のモジュールの全ての他のモジュールから切り離して原子炉トリップを論理的に決定する。

【００１１】

前の局面のうちのいずれかと組合せ可能な第１２の局面において、複数の機能的に独立したモジュールは、ＥＳＦコンポーネント毎に複数の独立したＥＳＦＡＳ作動投票モジュールを提供含む。

【００１２】

前の局面のうちのいずれかと組合せ可能な第１３の局面において、複数の機能的に独立したモジュールは、特定のＥＳＦコンポーネントに専用の複数のモジュールの全ての他のモジュールから切り離してＥＳＦＡＳ作動を論理的に決定する。

【００１３】

前の局面のうちのいずれかと組合せ可能な第１４の局面において、複数の機能的に独立したモジュールは、複数の安全機能モジュールを含む。

前の局面のうちのいずれかと組合せ可能な第２の局面において、複数の機能的に独立したモジュールは、複数の通信モジュールを含む。

【００１４】

前の局面のうちのいずれかと組合せ可能な第１５の局面において、複数の機能的に独立したモジュールは、複数の機器インタフェースモジュールを含む。

前の局面のうちのいずれかと組合せ可能な第１６の局面において、複数の機能的に独立したモジュールは、単一階層投票スキームにおいて原子炉トリップを論理的に決定する。

【００１５】

前の局面のうちのいずれかと組合せ可能な第１７の局面において、複数の機能的に独立

したモジュールは、複数階層投票スキームにおいて原子炉トリップを論理的に決定する。
前の局面のうちのいずれかと組合せ可能な第１８の局面において、複数階層投票スキームは２階層投票スキームを含む。
【００１６】
前の局面のうちのいずれかと組合せ可能な第１９の局面において、２階層投票スキームの第１の階層は、多数決投票スキームを含む。
前の局面のうちのいずれかと組合せ可能な第２０の局面において、多数決投票スキームは、３分の２投票スキームを含む。
【００１７】
前の局面のうちのいずれかと組合せ可能な第２１の局面において、２階層投票スキームの第２の階層は、非多数決投票スキームを含む。
前の局面のうちのいずれかと組合せ可能な第２２の局面において、第２の階層は、４分の２投票スキームを含む。
【００１８】
本開示に係る別の全体的な実装形態において、原子炉トリップを決定するための方法は、工学的安全施設作動システム（ＥＳＦＡＳ）又は原子炉トリップシステム（ＲＴＳ）のうちの一方から、原子炉保護システムの複数の機能的に独立したモジュールにおいて複数の入力を受信することと、複数の機能的に独立したモジュールによって、少なくとも部分的に複数の入力に基づいて、ＥＳＦＡＳ安全動作又は原子炉トリップの決定のうちの一方を論理的に決定することと、論理的な決定に基づいて、複数の機能的に独立したモジュールに通信可能に接続されたＥＳＦＡＳコンポーネントアクチュエータ又は原子炉トリップ遮断器のうちの一方を作動させることとを含む。
【００１９】
全体的な実装形態と組合せ可能な第１の局面は、更に、複数の機能的に独立したモジュールのうちの１つによって、複数の機能的に独立したモジュールのうちのいずれかの他のモジュールに対する単一の故障伝搬を制限することを含む。
【００２０】
前の局面のうちのいずれかと組合せ可能な第２の局面において、単一の故障は、単一のハードウェア故障、単一のソフトウェア故障、又は単一のソフトウェア生成論理故障のうちの少なくとも１つを含む。
【００２１】
前の局面のうちのいずれかと組合せ可能な第３の局面において、複数の機能的に独立したモジュールによって、少なくとも部分的に入力に基づいて、ＥＳＦＡＳ安全動作又は原子炉トリップの決定の一方を論理的に決定することは、複数の機能的に独立したモジュールによって、３重冗長化信号経路を通してＥＳＦＡＳ安全動作又は原子炉トリップの決定を論理的に決定することを含む。
【００２２】
前の局面のうちのいずれかと組合せ可能な第４の局面において、複数の機能的に独立したモジュールは、冗長ＲＴＳ投票部又は冗長ＥＳＦＡＳ投票部のうちの少なくとも一方を提供する。
【００２３】
前の局面のうちのいずれかと組合せ可能な第５の局面において、複数の機能的に独立したモジュールによって、少なくとも部分的に入力に基づいて、ＥＳＦＡＳ安全動作又は原子炉トリップの決定の一方を論理的に決定することは、複数の機能的に独立したモジュールによって、原子炉トリップコンポーネント毎の複数の独立したトリップ投票モジュールを通してＥＳＦＡＳ安全動作又は原子炉トリップの決定を論理的に決定することを含む。
【００２４】
前の局面のうちのいずれかと組合せ可能な第６の局面において、複数の機能的に独立したモジュールによって、少なくとも部分的に入力に基づいて、ＥＳＦＡＳ安全動作又は原子炉トリップの決定の一方を論理的に決定することは、複数の機能的に独立したモジュー

ルのうちの特定のモジュールによって、複数のモジュールの全ての他のモジュールから切り離してＥＳＦＡＳ安全動作又は原子炉トリップの決定を論理的に決定することを含む。

【００２５】

前の局面のうちいずれかと組合せ可能な第７の局面において、複数の機能的に独立したモジュールは、ＥＳＦコンポーネント毎の複数の独立したＥＳＦＡＳ作動投票モジュールを含み、方法は、更に、複数の機能的に独立したモジュールの特定のモジュールによって、特定のＥＳＦコンポーネントに専用の複数のモジュールの全ての他のモジュールから切り離してＥＳＦＡＳ作動を論理的に決定することを含む。

【００２６】

前の局面のうちのいずれかと組合せ可能な第８の局面において、複数の機能的に独立したモジュールは、複数の安全機能モジュール、複数の通信モジュール、及び複数の機器インタフェースモジュールを含む。

【００２７】

前の局面のうちのいずれかと組合せ可能な第９の局面において、複数の機能的に独立したモジュールによって、少なくとも部分的に入力に基づいて、ＥＳＦＡＳ安全動作又は原子炉トリップの決定のうちの一方を論理的に決定することは、複数の機能的に独立したモジュールによって、単一階層投票スキームにおいてＥＳＦＡＳ安全動作又は原子炉トリップの決定を論理的に決定することを含む。

【００２８】

前の局面のうちのいずれかと組合せ可能な第１０の局面において、複数の機能的に独立したモジュールによって、少なくとも部分的に入力に基づいて、ＥＳＦＡＳ安全動作又は原子炉トリップの決定のうちの一方を論理的に決定することは、複数の機能的に独立したモジュールによって、複数階層投票スキームにおいてＥＳＦＡＳ安全動作又は原子炉トリップの決定を論理的に決定することを含む。

【００２９】

前の局面のうちのいずれかと組合せ可能な第１１の局面において、複数階層投票スキームは２階層投票スキームを含む。

前の局面のうちのいずれかと組合せ可能な第１２の局面において、２階層投票スキームの第１の階層は、多数決投票スキームを含む。

【００３０】

前の局面のうちのいずれかと組合せ可能な第１３の局面において、多数決投票スキームは、３分の２投票スキームを含む。

前の局面のうちのいずれかと組合せ可能な第１４の局面において、２階層投票スキームの第２の階層は、非多数決投票スキームを含む。

【００３１】

前の局面のうちのいずれかと組合せ可能な第１５の局面において、第２の階層は、４分の２投票スキームを含む。

本開示に係る別の全体的な実装形態において、原子炉保護システムは、単一のモジュールへの単一の故障の移行を制限する複数の機能的に独立したモジュールを含む。

【００３２】

本開示に係る別の全体的な実装形態において、原子炉保護システムは、３つの型のモジュールだけを含み、それにより、作業ラインで交換可能なユニットの数を最小化する、複数の機能的に独立したモジュールを含む。

【００３３】

本開示に係る別の全体的な実装形態において、原子炉保護システムは、データバスを通ってデータが通過するスケジュールを決定する通信モジュールを含む複数の機能的に独立したモジュールを含む。

【００３４】

本開示に係る別の全体的な実装形態において、原子炉保護システムは、システムアーキテクチャを規定する原子炉トリップシステムを含み、そのシステムアーキテクチャでは、

例えば事故後監視機能ではなく、安全機能に排他的に関連する経路を通って、データが原子炉トリップシステムから制御室に送信される。

【００３５】

本開示に係る別の全体的な実装形態において、原子炉保護システムは、複数の機能的に独立したモジュールを含み、複数の機能的に独立したモジュールの各々は、システムにおける複数の原子炉トリップ遮断器の間で特定の原子炉トリップ遮断器に専用である。

【００３６】

本開示に係る別の全体的な実装形態において、原子炉保護システムは、複数の機能的に独立したモジュールを含み、複数の機能的に独立したモジュールの各々は、他のモジュールの全てと完全に独立に、原子炉トリップ／トリップなし決定又はＥＳＦＡＳ作動／作動なし決定を行う。

【００３７】

本開示に係る別の全体的な実装形態において、原子炉保護システムは、複数の機能的に独立したモジュールを含み、複数の機能的に独立したモジュールの各々は、システムにおける複数のＥＳＦＡＳ機器アクチュエータの間で特定のＥＳＦＡＳ機器アクチュエータに専用である。

【００３８】

本開示に係る別の全体的な実装形態において、原子炉保護装置は、原子炉安全システムから複数の入力を受信し、少なくとも部分的に複数の入力に基づいて、安全動作を論理的に決定するための手段と、少なくとも部分的に複数の入力に基づいて、安全動作決定を受信するための手段とを含む。

【００３９】

全体的な実装形態と組合せ可能な第１の局面において、安全動作決定を受信するための手段は、原子炉安全システムから複数の入力を受信し、安全動作を論理的に決定するための手段に通信可能に接続される。

【００４０】

前の局面のうちのいずれかと組合せ可能な第２の局面において、原子炉安全システムから複数の入力を受信し、安全動作を論理的に決定するための手段は、装置内の単一の故障伝搬に対する保護を提供する。

【００４１】

前の局面のうちのいずれかと組合せ可能な第３の局面において、原子炉安全システムは、工学的安全施設作動システム（ＥＳＦＡＳ）を備え、原子炉安全システムから複数の入力を受信し、安全動作を論理的に決定するための手段は、複数のＥＳＦＡＳ入力を受信し、少なくとも部分的にＥＳＦＡＳ入力に基づいて、ＥＳＦＡＳコンポーネント作動を論理的に決定する。

【００４２】

前の局面のうちのいずれかと組合せ可能な第４の局面において、原子炉安全システムから複数の入力を受信し、安全動作を論理的に決定するための手段は、冗長ＥＳＦＡＳ投票部を提供する。

【００４３】

前の局面のうちのいずれかと組合せ可能な第５の局面において、原子炉安全システムは、原子炉トリップシステム（ＲＴＳ）を備え、原子炉安全システムから複数の入力を受信し、安全動作を論理的に決定するための手段は、複数のＲＴＳ入力を受信し、少なくとも部分的にＲＴＳ入力に基づいて、ＲＴＳコンポーネント作動を論理的に決定する。

【００４４】

前の局面のうちのいずれかと組合せ可能な第６の局面において、原子炉安全システムから複数の入力を受信し、安全動作を論理的に決定するための手段は、冗長ＲＴＳ投票区分を備える。

【００４５】

前の局面のうちのいずれかと組合せ可能な第７の局面において、原子炉安全システムか

ら複数の入力を受信し、安全動作を論理的に決定するための手段は、装置内の単一のハードウェア故障伝搬に対する保護を提供する。

【００４６】

前の局面のうちのいずれかと組合せ可能な第８の局面において、原子炉安全システムから複数の入力を受信し、安全動作を論理的に決定するための手段は、装置内の単一のソフトウェア故障伝搬に対する保護を提供する。

【００４７】

前の局面のうちのいずれかと組合せ可能な第９の局面において、原子炉安全システムから複数の入力を受信し、安全動作を論理的に決定するための手段は、装置内の単一のソフトウェア生成論理故障伝搬に対する保護を提供する。

【００４８】

前の局面のうちのいずれかと組合せ可能な第１０の局面において、原子炉安全システムから複数の入力を受信し、安全動作を論理的に決定するための手段は、原子炉トリップ検知及び決定の３重冗長信号経路を備える。

【００４９】

前の局面のうちのいずれかと組合せ可能な第１１の局面において、原子炉安全システムから複数の入力を受信し、安全動作を論理的に決定するための手段は、原子炉トリップコンポーネント毎に複数の独立したトリップ投票モジュールを備える。

【００５０】

前の局面のうちのいずれかと組合せ可能な第１２の局面において、原子炉安全システムから複数の入力を受信し、安全動作を論理的に決定するための手段は、特定の原子炉トリップコンポーネントについて原子炉トリップを独立して決定する。

【００５１】

前の局面のうちのいずれかと組合せ可能な第１３の局面において、原子炉安全システムから複数の入力を受信し、安全動作を論理的に決定するための手段は、ＥＳＦコンポーネント毎に複数の独立したＥＳＦＡＳ作動投票モジュールを備える。

【００５２】

前の局面のうちのいずれかと組合せ可能な第１４の局面において、原子炉安全システムから複数の入力を受信し、安全動作を論理的に決定するための手段は、特定のＥＳＦコンポーネントについてＥＳＦＡＳ作動を独立して決定する。

【００５３】

前の局面のうちのいずれかと組合せ可能な第１５の局面において、原子炉安全システムから複数の入力を受信し、安全動作を論理的に決定するための手段は、複数の安全機能モジュールを備える。

【００５４】

前の局面のうちのいずれかと組合せ可能な第１６の局面において、原子炉安全システムから複数の入力を受信し、安全動作を論理的に決定するための手段は、複数の通信モジュールを備える。

【００５５】

前の局面のうちのいずれかと組合せ可能な第１７の局面において、原子炉安全システムから複数の入力を受信し、安全動作を論理的に決定するための手段は、複数の機器インタフェースモジュールを備える。

【００５６】

前の局面のうちのいずれかと組合せ可能な第１８の局面において、原子炉安全システムから複数の入力を受信し、安全動作を論理的に決定するための手段は、単一階層投票スキームにおいて原子炉トリップを論理的に決定する。

【００５７】

前の局面のうちのいずれかと組合せ可能な第１９の局面において、原子炉安全システムから複数の入力を受信し、安全動作を論理的に決定するための手段は、複数階層投票スキームにおいて原子炉トリップを論理的に決定する。

【００５８】
前の局面のうちのいずれかと組合せ可能な第２０の局面において、複数階層投票スキームは２階層投票スキームを備える。
前の局面のうちのいずれかと組合せ可能な第２１の局面において、２階層投票スキームの第１の階層は、多数決投票スキームを備える。
【００５９】
前の局面のうちのいずれかと組合せ可能な第２２の局面において、多数決投票スキームは、３分の２投票スキームを備える。
前の局面のうちのいずれかと組合せ可能な第２３の局面において、２階層投票スキームの第２の階層は、非多数決投票スキームを備える。
【００６０】
前の局面のうちのいずれかと組合せ可能な第２４の局面において、第２の階層は、４分の２投票スキームを備える。
本開示に係る原子炉保護システムの種々の実装形態は、以下の特徴の１つ、幾つか、又は全てを含み得る。例えば、原子炉保護システムは、システムにおける安全機能を無効化および／又は不能化し得るソフトウェア又はソフトウェア生成論理エラーによって引き起こされる共通原因故障（ＣＣＦ）を緩和し得る。別の例として、原子炉保護システムは、独立性、冗長性、決定論、多層化多様性、試験可能性、及び診断を含む主要属性を組み込んでもよい。原子炉保護システムは、原子炉が安全状態で維持されることを保証し得る。別の例として、原子炉保護システムは、特定の機能に専用の個々の論理エンジンに実装される機能性を有する対称アーキテクチャを通して増加した簡素性を有してもよい。更に別の例として、原子炉保護システムは、単純な決定論的プロトコルに基づく、かつ冗長経路を介して通信される、アーキテクチャ内での通信を容易にし得る。
【００６１】
本明細書で述べる主題の１つ又は複数の実装形態の詳細は、添付図面及び以下の説明において述べられる。本主題の他の特徴、局面、及び利点は、説明、図面、及び請求項から明らかになるであろう。
【図面の簡単な説明】
【００６２】
【図１】複数の原子力システムと、計装及び制御（Ｉ＆Ｃ）システムとを含むシステムの例示的な実装形態のブロック図を図示している。
【図２Ａ】原子力システム用のＩ＆Ｃシステムのモジュール保護システム（ＭＰＳ）のブロック図を図示している。
【図２Ｂ】原子力システム用のＩ＆Ｃシステムのモジュール保護システム（ＭＰＳ）のブロック図を図示している。
【図３Ａ】原子力システムのためのＩ＆ＣシステムのＭＰＳのトリップ決定ブロックのブロック図を図示している。
【図３Ｂ】原子力システムのためのＩ＆ＣシステムのＭＰＳの工学的安全施設作動システム（ＥＳＦＡＳ）のブロック図を図示している。
【図４Ａ－４Ｂ】Ｉ＆Ｃシステムがその意図する安全機能を実行することができることを保証する、ＭＰＳ内のソフトウェア又はソフトウェア論理ベース共通原因故障を緩和する多層化多様性戦略を図示する例示的なチャートを図示している。
【図５】原子力システムのためのＩ＆ＣシステムのＭＰＳの安全機能モジュール（ＳＦＭ）のブロック図を図示している。
【図６】原子力システムのためのＩ＆ＣシステムのＭＰＳの通信モジュール（ＣＭ）のブロック図を図示している。
【図７】原子力システムのためのＩ＆ＣシステムのＭＰＳの機器インタフェースモジュール（ＥＩＭ）のブロック図を図示している。
【図８】１つ又は複数のＳＦＭ、ＥＩＭ、及びＣＭを通信可能に接続する原子炉保護システムの筐体の例示的な実施形態を図示している。

【図９Ａ】ＳＦＭ、ＣＭ、及びＥＩＭの１つ又は複数を利用する、トリップ決定レベル相互接続、ＲＴＳレベル相互接続、及びＥＳＦＡＳレベル相互接続のブロック図を図示している。
【図９Ｂ】ＳＦＭ、ＣＭ、及びＥＩＭの１つ又は複数を利用する、トリップ決定レベル相互接続、ＲＴＳレベル相互接続、及びＥＳＦＡＳレベル相互接続のブロック図を図示している。
【図９Ｃ】ＳＦＭ、ＣＭ、及びＥＩＭの１つ又は複数を利用する、トリップ決定レベル相互接続、ＲＴＳレベル相互接続、及びＥＳＦＡＳレベル相互接続のブロック図を図示している。
【図１０】原子力システムのためのＩ＆Ｃシステムのためのの多様性分析ダイアグラムを図示している。
【図１１】防護の４つの階層へのＭＰＳブロックの例示的な分離のブロック図を図示している。
【発明を実施するための形態】
【００６３】
［詳細な説明］
図１は、複数の原子力システム１５０と、原子炉計装及び制御（Ｉ＆Ｃ）システム１３５とを含むシステム１００の例示的な実装形態を図示している。一般的に、Ｉ＆Ｃシステム１３５は、自動始動信号、自動及び手動制御信号、並びに監視及び指示ディスプレイを提供して、システム１００における故障状態の結果を防止又は緩和する。Ｉ＆Ｃシステム１３５は、正常な原子炉制御と、定常状態及び過渡的電力運転中に原子力システム１５０の安全でない原子炉運転に対しての保護とを提供する。正常運転中、計装は、種々のプロセスパラメータを測定し、その信号をＩ＆Ｃシステム１３５の制御システムに送信する。異常運転及び事故状態中、計装は、信号をＩ＆Ｃシステム１３５の複数の部分（モジュール保護システム（ＭＰＳ）１４５の部分である、例えば（例えば、事故の影響を緩和するための）原子炉トリップシステム（ＲＴＳ）１４７及び工学的安全施設作動システム（ＥＳＦＡＳ）１４８）に送信して、所定の設定点に基づいて保護動作を始動する。
【００６４】
図１において、システム１００は、Ｉ＆Ｃシステム１３５に電気的に接続される複数の原子力システム１５０を含む。３つの原子力システム１５０だけがこの例では示されるが、システム１００内に含まれるか又はシステム１００に接続されるより少ないか又はより多い（例えば、６、９、１２、又はその他の数の）システム１５０が存在してもよい。１つの好ましい実装形態において、システム１００内に含まれる１２の原子力システム１５０が存在してもよく、原子力システム１５０の１つ又は複数は、以下で更に述べるように、モジュール式の軽水炉を含む。
【００６５】
各原子力システム１５０に関して、また、明示的に示されないが、原子炉炉心は熱を提供することができ、その熱が利用されて、（例えば、沸騰水型原子炉の場合と同様に）１次冷却ループ内で又は（例えば、加圧水型原子炉の場合と同様に）２次冷却ループ内で水を沸騰させる。例えば蒸気等の気化した冷却剤が使用されて、１つ又は複数のタービンを駆動してもよく、タービンは熱ポテンシャルエネルギーを電気エネルギーに変換する。凝縮された後、冷却剤は、その後、戻されて、原子炉炉心からより多くの熱エネルギーを再び除去する。原子力システム１５０は、システム内の故障に関連する危険を最小にするため監視及び保護機能を必要とする任意のシステムの一例である。
【００６６】
各原子炉システム１５０の特定の例示的な実装形態において、炉心は、円柱状又はカプセル状の原子炉容器の底部に配置される。炉心は、おそらく数年以上の期間にわたって起こり得る制御された反応を生成する或る量の核分裂性物質を含む。図１に明示的に示さないが、制御棒が使用されて、炉心内の核分裂速度を制御してもよい。制御棒は、銀、インジウム、カドミウム、ホウ素、コバルト、ハフニウム、ジスプロシウム、ガドリニウム、

サマリウム、エルビウム、及びユーロピウム、又はそれらの合金及び化合物を含み得る。しかしながら、これらは、多くの考えられる制御棒材料のうちの少数に過ぎない。受動的運転システムを有するように設計される原子炉では、正常運転中に又はたとえ緊急状態においても、オペレータの介入又は監督なしで、少なくとも予め規定された或る期間の間、原子炉の安全運転が維持されることを保証するのに物理法則が利用される。

【００６７】

複数の実装形態において、円筒状又はカプセル状の格納容器は、原子炉容器を囲み、原子炉ベイ内で、例えば水線未満等、原子炉プール内に部分的に又は完全に浸漬される。原子炉容器と格納容器との間の容積は、部分的に又は完全に真空排気されて、原子炉容器から原子炉プールへの熱伝達を低減する。しかしながら、他の実装形態において、原子炉容器と格納容器との間の容積を、原子炉と格納容器との間の熱伝達を増加させる気体及び／又は液体で少なくとも部分的に充填してもよい。格納容器は、原子炉ベイのベースのスカート上に載ってもよい。

【００６８】

特定の実装形態において、炉心は、ホウ素又は他の添加剤を含み得る、例えば水等の液体内に浸漬され、この液体は、炉心の表面と接触した後にチャネル内を上昇する。冷却剤は、熱交換器の上部にわたって移動し、原子炉容器の内壁に沿って、対流によって下方に引かれ、ひいては、冷却剤が熱を熱交換器に与える。原子炉容器の底部に達した後、炉心との接触は、冷却剤を加熱することをもたらし、冷却剤は、再びチャネルを通って上昇する。

【００６９】

原子炉容器内の熱交換器は、チャネルの少なくとも一部分に巻付く任意の数の螺旋コイルを表し得る。別の実装形態において、異なる数の螺旋コイルが、対向する方向にチャネルに巻付いてもよく、例えば、第１の螺旋コイルが反時計方向に螺旋状に巻付く一方、第２の螺旋コイルが時計方向に螺旋状に巻付く。しかしながら、異なるように構成された、及び／又は異なるように配向された熱交換器の使用を何ものも妨げず、実装形態は、この点に関して制限されない。

【００７０】

図１において、原子炉モジュールの正常運転は、加熱された冷却剤がチャネルを通って上昇し、熱交換器と接触するように進む。熱交換器と接触した後、冷却剤は、吸熱プロセスを誘起する方法で原子炉容器の底部に向かって沈む。図１の例において、原子炉容器内の冷却剤は、大気圧を超える圧力のままであり、ひいては、冷却剤が、気化する（例えば、沸騰する）ことなく高温を維持することを可能にする。

【００７１】

熱交換器内の冷却剤の温度が上がるにつれて、冷却剤は沸騰を始め得る。熱交換器内の冷却剤が沸騰し始めると、例えば蒸気等の気化した冷却剤を１つ又は複数のタービンを駆動するのに使用することができ、タービンは、蒸気の熱ポテンシャルエネルギーを電気エネルギーに変換する。凝縮された後、冷却剤は、熱交換器のベースの近くの場所に戻される。

【００７２】

図１の原子力システム１５０の正常運転中、原子力システムの種々の性能パラメータを、原子力システム１５０内の種々の場所に配置された、例えばＩ＆Ｃシステム１３５といったセンサによって監視してもよい。原子力システム内のセンサは、システム温度、システム圧力、１次及び／又は２次冷却剤レベル、及び中性子束を測定してもよい。これらの測定値を示す信号を、原子力システムの外部で通信チャネルによってＩ＆Ｃシステム１３５のインタフェースパネルにレポートしてもよい。

【００７３】

図示されたＩ＆Ｃシステム１３５は、一般的に、主制御室１４０、モジュール（又は原子炉）保護システム（ＭＰＳ）１４５、及び非安全モジュール制御システム（ＭＣＳ）１５５を含む。主制御室１４０は、各原子力システム１５０のための制御装置及び計器のセ

ット１４１を含む。制御装置及び計器の各セット１４１は、手動１Ｅ制御装置１４２、１Ｅ計器１４３、並びに非１Ｅ制御装置及び計器１４４を含む。幾つかの局面において、「１Ｅ」は、例えば原子力規制委員会規制ガイド１．３２によって承認されたＩＥＥＥ規格３０８－２００１のセクション３．７における１Ｅスキームを規定する要件等のような規制要件を指すことができ、１Ｅスキームは、緊急原子炉停止、格納容器隔離、炉心冷却、及び、格納容器及び原子炉の熱除去にとって必須の、又は別途、環境内への放射性物質の著しい放出を防止するときに必須の、電気機器及びシステムの安全性分類を規定する。通常、或る制御装置及び計器（例えば、手動１Ｅ制御装置１４２及び１Ｅ計器１４３）は「１Ｅ」適格であってもよく、一方、他の制御装置及び計器（例えば、非１Ｅ制御装置及び計器１４４）は「１Ｅ」適格でなくてもよい。

【００７４】

非１Ｅ制御装置及び計器１４４は、ＭＣＳ１５５と双方向通信状態にある。ＭＣＳ１５５は、原子力システム１５０の非安全部分の制御及び監視を提供してもよい。一般的に、ＭＣＳ１５５は、運転上の過渡状態を抑制して、ユニットトリップを防止し、運転の中でもとりわけ定常状態ユニット運転を再確立する。

【００７５】

ＭＰＳ１４５は、図１に示すように、手動１Ｅ制御装置１４２及び１Ｅ計器１４３とそれぞれ一方向通信状態にある。ＭＰＳ１４５は、一般的に、安全動作を始動して、設計基準事象の結果を緩和する。ＭＰＳ１４５は、一般的に、原子炉停止を始動するために必要とされる、センサから最終的な作動デバイス（電力源、センサ、信号調節器、始動回路、論理、バイパス、制御ボード、相互接続部、及び作動デバイス）までの（ハードウェア、ソフトウェア、及びファームウェアを含む）全ての機器を含む。

【００７６】

ＭＰＳ１４５は、ＲＴＳ１４７及びＥＳＦＡＳ１４８を含む。ＲＴＳ１４７は、幾つかの局面において、原子炉トリップを生成するために利用され得るプラントパラメータを監視するため、独立した測定チャネルを有する４つの独立した分離グループ（例えば、同じクラス－１Ｅ電気チャネル指定（Ａ、Ｂ、Ｃ、又はＤ）を有するプロセスチャネルの物理的分類であって、別個でかつ独立した給電部及びプロセス計装送信機が設けられ、また、そのグループのそれぞれが、他のグループと物理的にかつ電気的に独立している、プロセスチャネルの物理的分類）を含む。各測定チャネルは、パラメータが所定の設定点を超えるとトリップする。ＲＴＳ１４７の一致論理は、どの単一の故障も、必要とされるときに原子炉トリップを妨げる可能性がなく、かつ、単一の測定チャネルにおけるどの故障も、不必要な原子炉トリップを生成する可能性がないように設計されてもよい。

【００７７】

ＥＳＦＡＳ１４８は、幾つかの局面において、独立した測定チャネルを有する４つの独立した分離グループを含み、独立した測定チャネルはプラントパラメータを監視し、プラントパラメータは、工学的安全施設（ＥＳＦ）機器の運転を起動するのに使用され得る。各測定チャネルは、パラメータが所定の設定点を超えるとトリップする。ＥＳＦＡＳ１４８の一致論理は、どの単一の故障も、必要とされるときに保障措置作動を妨げる可能性がなく、かつ、単一の測定チャネルにおけるどの単一の故障も、不必要なセーフガード作動を生成する可能性がないように設計されてもよい。

【００７８】

システム１００は、ＮＵＲＥＧ／ＣＲ－６３０３に規定されるように、防護の４つの階層、例えば、原子炉を運転するため、又は、原子炉を停止し原子炉を冷却するために原子炉に取り付けられた計装及び制御システムの配置構成に対する深層防護の原理の特定の適用を含んでもよい。特に、４つの階層は、制御システム、原子炉トリップ又はスクラムシステム、ＥＳＦＡＳ、及び、監視及び計器システム（例えば、最も遅くかつ最も柔軟性のある防護の階層であって、他の３つの階層に名目的に割り当てられる機器を運転するために必要とされる、クラス１Ｅと非クラス１Ｅとの双方の手動制御装置、モニター、及び計器を含む、防護の階層）である。

【００７９】
制御システム階層は、通常、ＭＣＳ１５５（例えば、非クラス１Ｅ手動又は自動制御機器）を含み、ＭＣＳ１５５は、安全でない運転レジームに向かう原子炉暴走を定期的に防止し、また、一般的に、原子炉を安全発電運転領域内で運転するのに使用される。計器、アナンシエータ、及びアラームは、制御階層に含まれてもよい。原子炉制御システムは、通常、特定の規則及び／又は要求、例えば、遠隔停止パネルのための要求を満たす何らかの機器を含む。制御システム階層によって実行される原子炉制御機能はＭＣＳ１５５に含まれる。ＭＣＳ１５５は、例えば、運転限界内でシステム１００を維持して、原子炉トリップ又はＥＳＦ作動についての必要性を回避する機能を含む。

【００８０】
原子炉トリップシステム階層は、通常、ＲＴＳ１４７、例えば、制御されない暴走に応答して炉心反応を急速に低減するように設計された安全機器を含む。この階層は、通常、潜在的な又は実際の暴走を検出するための計装、原子炉制御棒を急速にかつ完全に挿入するための機器及びプロセスからなり、また同様に、或る化学的中性子減速システム（例えば、ホウ素注入）を含んでもよい。図示されるように、原子炉トリップ階層によって実行される自動原子炉トリップ機能は、ＭＰＳ１４５に（例えば、ＲＴＳ１４７に）含まれる。

【００８１】
ＥＳＦＡＳ階層は、通常、ＭＰＳ１４５の一部であるＥＳＦＡＳモジュール１４８を含む。ＥＳＦＡＳモジュール１４８内に実装されるＥＳＦＡＳ階層は、通常、熱を除去するか又はそうでなければ放射性物質放出に対する３つの物理的障壁（例えば、原子炉燃料棒被覆管、原子炉容器、及び原子炉格納）の完全性を維持するのを補助する安全機器を含む。この階層は、例えば緊急時原子炉冷却、圧力逃がし又は減圧、隔離、及び、ＥＳＦ機器が運転するために必要とされる種々の支持システム（例えば、緊急時発電機）又はデバイス（弁、モータ、ポンプ）の制御といった機能等についての必要性を検出し、それを実行する。

【００８２】
監視及び計器システム階層は、通常、主制御室１４０を含み、また、幾つかの局面において、最も遅くまた同様に最も柔軟性がある防護の階層である。他の３つの階層のように、（例えば、システム１００の）人間オペレータは、自分のタスクを実行するために正確なセンサ情報に依存するが、情報、時間、及び手段が与えられると、予期しない事象に反応するため、前もって指定されていない論理的演算を実行できる。監視及び指示階層は、他の３つの階層に（例えば、手動１Ｅ制御装置１４２、１Ｅ計器１４３、及び非１Ｅ制御装置及び計器１４４を通して）名目上割り当てられた機器を運転するために必要とされるクラス１Ｅ及び非クラス１Ｅ制御装置、モニター、及び計器を含む。監視及び計器システム階層によって要求される機能は、主制御室内の手動制御装置、ディスプレイ、及び計器によって提供され、ＭＣＳ１５５及びＭＰＳ１４５からの情報を含む。安全監視、手動原子炉トリップ、及び手動ＥＦＳ作動機能はＭＰＳ１４５に含まれる。ＭＣＳ１５５は、非安全監視及び手動制御を提供して、正常プラント運転中に運転限界を維持する。

【００８３】
防護の４つの階層を含むことに加えて、システム１００は、複数レベルの多様性を含む。特に、Ｉ＆Ｃ多様性は、異なる技術、論理、又はアルゴリズムを使用して変数を測定するか又は作動手段を提供するという原理であり、想定プラント状態に対応する多様な方法を提供する。ここで、多様性は、異なる技術、論理、又はアルゴリズムを使用して異なるパラメータを検知する計装システム、又は、作動手段の原理に適用されて、重大事象を検出し、重大事象に応答する幾つかの方法を提供する。多様性は、深層防護の原理に相補的であり、特定のレベル又は深度の防護が、必要とされるときに作動されることになる機会を増加させる。一般的に、６つの多様性の属性、すなわち、人間多様性、設計多様性、ソフトウェア多様性、機能多様性、信号多様性、及び機器多様性が存在する。本開示でより詳細に論じるように、ＭＰＳ１４５は、ＭＰＳ１４５における共通原因故障（例えば、ハ

ードウェアアーキテクチャによって達成される冗長性を無効にし得るソフトウェアエラー又はソフトウェア生成論理によって引き起こされる故障）の影響を緩和するために、６つの多様性の属性を組み込んでもよい。

【００８４】

一般的に、人間多様性は、システム開発ライフサイクル全体にわたる人間生成の過失（例えば、誤り、誤解釈、エラー、構成失敗）に対処することに関連し、また、ライフサイクルプロセスの実行における不同性を特徴とする。

【００８５】

一般的に、設計多様性は、同じか又は類似の問題を解決するための、ソフトウェア及びハードウェアを含む異なるアプローチの使用である。ソフトウェア多様性は、設計多様性の特別な場合であり、その考えられる重要性及びその考えられる欠点のために別々に述べられる。設計多様性についての理論的解釈は、異なる設計が異なる故障モードを有し、同じ共通影響を受けないことである。

【００８６】

一般的に、ソフトウェア多様性は、例えば、原子炉がいつトリップされるべきかを決定するための２つの別々に設計されたプログラムを使用して、同じ安全目標を達成するための、異なる主要職員を有する異なるソフトウェア開発グループによって設計され、実装される異なるソフトウェアプログラムの使用である。

【００８７】

一般的に、機能多様性は、異なる物理的又は論理的機能を実行する２つのシステム（例えば、システム１００内のサブシステム）を指すが、２つのシステムは、オーバラップする安全効果を有してもよい。

【００８８】

一般的に、信号多様性は、保護動作を始動する異なるプロセスパラメータの使用であり、保護動作において、そのパラメータのうちのいずれも、他のパラメータが正しく検出されない場合でも、異常状態を独立して示し得る。

【００８９】

一般的に、機器多様性は、類似の安全機能（例えば、必要とされる全ての保護動作をＲＴＳ又はＥＳＦが完了することか、必要とされる全ての保護動作を補助的に支持する機能が完了することか、又は両方によって達成され得る、設計基準事象について確立された許容限度内にプラントパラメータを維持するのに必須のプロセス又は条件のうちの１つ）を実行するための異なる機器の使用である。この場合、「異なる」は、共通原因故障に対する脆弱性を著しく減少させるほどに十分に違っていることを意味してもよい。

【００９０】

幾つかの局面において、ＭＰＳ１４５は、連続的な（又は部分的に連続的な）自己試験及び定期的な監視試験の組合せを組み込んでもよい。こうした試験戦略は、検出可能な全ての故障が特定され、（例えば、主制御室１４０を通して）ステーション職員に通知されることを保証し得る。自己試験機能は、システム状態が連続的に（又は部分的に）監視されることを保証する包括的診断システムを提供してもよい。検出可能な全ての故障は、ステーション職員に通知されてもよく、故障の影響の指示が提供されて、システムの全体の状態を判定してもよい。自己試験機能は、分離グループ及び分割の独立性を維持する。自己試験機能は、システムの完全性が常に維持されることを保証する。

【００９１】

幾つかの局面において、（以下でより詳細に述べる）ＭＰＳ１４５内の各サブモジュールは、モジュール内の単一の故障を検出するように設計された高い故障検出範囲を提供する自己試験機能を含んでもよい。これは、故障を検出するのに必要とされる時間を最小にすることができ、安全及びシステム可用性に対する利益を提供する。システムが正常運転中であるとき、自己試験は、例えば応答時間等の安全機能の性能に影響を及ぼすことなく進む。

【００９２】

自己試験機能は、アクティブ論理及び非アクティブ論理（例えば、安全機能が作動することを必要とされるときだけにアクティブとなる論理）の双方においてほとんどの故障を検出することが可能であり、未検出故障を有することを回避し得る。故障検出及び指示は、ＭＰＳサブモジュールレベルにおいて起こり、プラント職員が、置換される必要があるＭＰＳサブモジュールを容易に特定することを可能にする。

【００９３】

周期的オンライン監視試験能力が組み込まれて、全ての機能試験及びチェック、較正検証、並びに時間応答測定が検証されることを保証してもよい。周期的監視試験はまた、継続的自己試験機能を検証する。

【００９４】

ＭＰＳ１４５内の自己試験及び周期的監視試験機能は、全てのプラント運転モードについて実行される安全機能に相応する稼働中試験可能性のために設計されてもよい。性能自己試験及び監視試験は、暫定試験セットアップを全く必要としない。試験機能は、システムの設計に固有であってもよく、安全機能論理及びデータ構造に最小の複雑さを付加してもよい。バイパス条件の継続的指示は、（１）プラントの正常運転中に自己試験によってフォールトが検出される場合、又は、（２）安全機能の或る部分が、バイパスされるか、又は、試験について故意に運転不能にされる場合に行われる。バイパス条件が取り除かれると、バイパスの指示が除去される。これは、バイパスされた安全機能がサービスに適切に戻されたことをプラント職員が確認できることを保証し得る。

【００９５】

ＭＰＳ１４５についての診断データは、各分離グループ及び分割についてメンテナンスワークステーション（ＭＷＳ）に提供される。ＭＷＳは、機器に接近して配置されて、トラブルシューティング活動を容易にしてもよい。ＭＰＳとＭＷＳとの間のインタフェースは、光学的に絶縁された一方向診断インタフェースであってもよい。全ての診断データは、物理的に離れた通信経路によって通信されてもよく、診断機能が安全機能と独立であることを保証し得る。更に、診断データを、長期格納のために、中央ヒストリアンに送信され得る。これは、システム運転の履歴分析を実行する手段を提供する。

【００９６】

診断システムは、設置されたモジュールのリストを維持してもよい。リストは、システム内でアクティブである設置されたモジュールと継続的に比較されて、モジュールの欠如又は正しくないモジュールが設置されることを予防してもよい。

【００９７】

全てのＭＰＳ安全データ通信は、データ完全性を高めるためにエラー検出を有するように設計されてもよい。プロトコル機能は、通信が、送信故障を検出する能力によってロバストでかつ信頼性があることを保証する。類似のデータ完全性機能が使用されて、診断データを転送してもよい。

【００９８】

図２Ａ～２Ｂは、原子力システム１５０のためのＩ＆Ｃシステムのモジュール保護システム（ＭＰＳ）２００のブロック図を図示している。幾つかの実装形態において、ＭＰＳ２００は、図１に示されたＭＰＳ１４５に類似するか又はそれと同一であってもよい。一般的に、図示されたＭＰＳ２００は、センサ及び検出器の４つの分離グループ（例えば、センサ２０２ａ～２０２ｄ）、信号調節及び信号調節器の４つの分離グループ（例えば、信号調節器２０４ａ～２０４ｄ）、トリップ決定の４つの分離グループ（例えば、トリップ決定２０８ａ～２０８ｄ）、ＲＴＳ投票及び原子炉トリップ遮断器の２つの区分（例えば、区分Ｉ　ＲＴＳ投票２１４及び区分ＩＩ　ＲＴＳ投票２１６）、及び、工学的安全施設作動システム（ＥＳＦＡＳ）投票及び工学的安全施設（ＥＳＦ）機器の２つの区分（例えば、区分Ｉ　ＥＳＦＡＳ投票２１２及びＥＳＦ機器２２４並びに区分ＩＩ　ＥＳＦＡＳ投票２１８及びＥＳＦ機器２２６）を含む。

【００９９】

一般的に、センサ２０２ａ～２０２ｄは、例えば圧力、温度、レベル、及び中性子束等

の異なるプロセスパラメータを測定することを担当するプロセスセンサを含む。そのため、原子力システム１５０の各プロセスパラメータは、異なるセンサを使用して測定され、異なる論理エンジンによって実行される異なるアルゴリズムによって処理される。幾つかの局面において、中性子束センサは、フルパワーの１２０パーセントまでの停止条件による、炉心からの中性子束を測定することを担当する。ソース範囲、中間範囲、及びパワー範囲を含む、３つの型の中性子束センサを、ＭＰＳ２００内で使用してもよい。

【０１００】

一般的に、信号調節器２０４ａ～２０４ｄは、センサ２０２ａ～２０２ｄから測定値を受信し、測定値を処理し、出力２０６ａ～２０６ｄを提供する。幾つかの局面において、信号調節器２０４ａ～２０４ｄに対するセンサ２０２ａ～２０２ｄの相互接続部は、専用銅線又は何らかの他の信号送信方法であってもよい。

【０１０１】

信号調節器２０４ａ～２０４ｄはそれぞれ、（例えば、センサ入力の数に応じて任意の数のモジュールを示す）図３Ａに示された複数の入力モジュール２７０ａ～２７０ｎからなってもよく、入力モジュール２７０ａ～２７０ｎは、センサ２０２ａ～２０２ｄからのフィールド入力を調節し、測定し、フィルタリングし、サンプリングすることを担う。各入力モジュール２７０ａ～２７０ｎは、例えば２４Ｖ又は４８Ｖデジタル入力、４～２０ｍＡアナログ入力、０～１０Ｖアナログ入力、抵抗熱検出器入力、又は熱電対入力等の特定の入力型に専用であってもよい。

【０１０２】

各入力モジュール２７０ａ～２７０ｎは、アナログ回路及びデジタル回路からなってもよい。アナログ回路は、アナログ電圧又はアナログ電流をデジタル表現に変換することを担う。アナログ回路は信号調節回路構成とも称される。各入力モジュール２７０ａ～２７０ｎのデジタル部分を、論理エンジン内に配置してもよい。論理エンジンは、全入力モジュール制御、サンプル及びホールドフィルタリング、完全性チェック、自己試験、及びデジタルフィルタリング機能を実行する。センサ出力のデジタル表現は、幾つかの例ではシリアルインタフェースを使用して、出力２０６ａ～２０６ｄを通して信号調節器２０４ａ～２０４ｄからトリップ決定２０８ａ～２０８ｄまで通信される。

【０１０３】

同様に図３Ａを参照すると、トリップ決定２０８ａ～２０８ｄは、一般的に、上述したように、信号調節器２０４ａ～２０４ｄからシリアルインタフェースを介してデジタルフォーマットでセンサ入力値を受信する。トリップ決定２０８ａ～２０８ｄはそれぞれ、（図５を参照してより完全に述べる）独立した安全機能モジュール（ＳＦＭ）２７２ａ～２７２ｎからなり、そこで、特定のモジュールが安全機能の１つのセットを実装する（例えば、セットは、特定のプロセスパラメータに関連する単一の安全機能又は複数の安全機能であってもよい）。例えば、安全機能のセットは、例えば同じ圧力入力からの高いトリップ及び低いトリップ等の、主要変数に関連する機能のグループからなってもよい。各ＳＦＭ２７２ａ～２７２ｎは、安全機能の１つのセットを実装することに専用の固有の論理エンジンを含む。これは、安全機能の全ての他のセットと全く異なる安全機能の各セットのゲートレベル実装をもたらす。

【０１０４】

センサ入力値（例えば、出力２０６ａ～２０６ｄ）は、決定論的経路を介して通信されてもよく、各トリップ決定２０８ａ～２０８ｄ内の特定のＳＦＭ２７２ａ～２７２ｎに提供される。その後、これらの入力値は工学単位に変換されて、どんな安全機能又は安全機能のセットがその特定のＳＦＭ２７２ａ～２７２ｎ上に実装されるかを決定してもよい。トリップ決定２０８ａ～２０８ｄは、これらの工学単位値を、幾つかの例では、絶縁された送信のみの光ファイバ接続を介して制御システムに提供する。

【０１０５】

各トリップ決定２０８ａ～２０８ｄにおけるＳＦＭは、必要である場合、所定の設定点に基づいて原子炉トリップ決定を行い、トリップ要求又はトリップなし要求信号を、絶縁

された、また幾つかの事例では３重冗長性があり送信のみのシリアル接続によって各ＲＴＳ区分（例えば、それぞれ、区分Ｉ及びＩＩのＲＴＳ投票２１４及び２１６）に提供する。ＳＦＭはまた、必要である場合、所定の設定点に基づいてＥＳＦＡＳ作動決定を行い、作動要求又は作動しない要求信号を、絶縁された、幾つかの事例では３重冗長性があり送信のみのシリアル接続によって各ＥＳＦＡＳ区分（例えば、それぞれ、区分Ｉ及びＩＩのＥＳＦＡＳ投票２１２及び２１８）に提供する。

【０１０６】

図３Ａ～３Ｂに示すように、例えば、特定のトリップ決定２０８ａは、トリップ要求又はトリップなし要求信号を、出力２７４ａを通してＥＳＦＡＳ投票２１２に、また、出力２７４ｂを通してＥＳＦＡＳ投票２１８に提供する。トリップ決定２０８ａは、トリップ要求又はトリップなし要求信号を、出力２７６ａを通してＲＴＳ投票２１４に、また、出力２７６ｂを通してＲＴＳ投票２１６に提供する。これらの出力はまた、それぞれ、トリップ決定２０８ａ～２０８ｄからの出力２１０ａ～２１０ｄとして、図２Ａに全体的に示される。

【０１０７】

図３Ａに更に示されるように、例えば、特定のトリップ決定２０８ａは、トリップ要求又はトリップなし要求信号を、監視及び指示（Ｍ＆Ｉ）出力２７８ａ及び２７８ｂ（１区分について１つ）並びに非１Ｅ出力２８０に提供する。出力２７８ａ及び２７８ｂは、非安全制御機能についてプロセス情報をＭＣＳに提供する。出力２８０は、プロセス情報及びトリップ状態情報を非１Ｅ制御装置及び計器１４４に提供する。

【０１０８】

図２Ａに戻ると、各ＲＴＳ区分（例えば、区分ＩのためのＲＴＳ投票２１４及び区分ＩＩのためのＲＴＳ投票２１６）は、絶縁され、また幾つかの局面では冗長性（例えば、２重、３重、又はその他）がある受信のみのシリアル接続２１０ａ～２１０ｄによって、上述したようにトリップ決定２０８ａ～２０８ｄから入力を受信する。トリップ入力は、トリップ決定２０８ａ～２０８ｄからの２つ以上の原子炉トリップ入力が自動原子炉トリップ出力信号を出力２２８ａ～２２８ｄ及び２３０ａ～２３０ｄ上に（各区分について適宜）生成するようにＲＴＳ投票論理において組み合せられ、自動原子炉トリップ出力信号は、それぞれの区分に関連する（図２Ｂに示す）８つの原子炉トリップ遮断器（ＲＴＢ）のうちの４つについてトリップコイルを作動させる。換言すれば、ＲＴＳ投票論理は、ＭＰＳ２００のこの例示的な実装形態において、「４分の２」論理に関して働き、原子炉「トリップ」が必要であることを４つのトリップ決定２０８ａ～２０８ｄのうちの少なくとも２つが示す場合、トリップ信号がＲＴＢ２６４ａ～２６４ｄ及び２６６ａ～２６６ｄのそれぞれに送信されることを意味する。この遮断器構成は、ＭＰＳ２００の安全でかつ簡単なオンライン試験を可能にする。

【０１０９】

手動トリップ２５０ａは、（区分Ｉのための）ＲＴＢ２６６ａ～２６６ｄの直接トリップを提供し、手動トリップ２５０ｂは、（区分ＩＩのための）ＲＴＢ２６４ａ～２６４ｄの直接トリップを提供すると共に、自動作動、（区分Ｉのための）手動トリップ２３４、及び（区分ＩＩのための）手動トリップ２３６に入力して、シーケンスが維持されることを保証する。

【０１１０】

更に図示されるように、各ＲＴＢ２６４ａ～２６４ｄ及び各ＲＴＢ２６６ａ～２６６ｄは、入力として、手動トリップ２５０ａ及び２５０ｂを含む。そのため、双方の手動トリップ２５０ａ及び２５０ｂ（例えば、区分Ｉ及びＩＩについての各手動トリップ）が始動される場合、電力入力２６０は、入力２３０ａ～２３０ｄ及び入力２２８ａ～２２８ｄの状態（例えば、トリップ又はトリップなし）によらず、電力出力２６２に送信されないことになる。

【０１１１】

ＥＳＦＡＳ投票及び論理は、例示的な実装形態では、どの単一の故障も、必要とされる

ときにセーフガード作動を妨げる可能性がなく、かつ、トリップ決定信号（例えば、２０１ａ～２１０ｄ）内のどの単一の故障も、不必要なセーフガード作動を生成する可能性がないように配置される。ＥＳＦＡＳシステムは、例えば緊急時炉心冷却システム及び崩壊熱除去システム等のクリティカルシステムの自動始動及び手動始動の双方を提供してもよい。

【０１１２】

各ＥＳＦＡＳ投票２１２／２１８は、入力２０１ａ～２１０ｄを、絶縁された３重冗長性があり受信のみの光ファイバ（又は他の通信技法）接続によってトリップ決定２０８ａ～２０８ｄから受信する。作動論理及び投票は、ＥＳＦＡＳ投票２１２／２１８内で起こる。ＥＳＦＡＳ投票２１２／２１８は、作動が必要であると判定すると、ＥＳＦＡＳ投票２１２／２１８は、適切なＥＳＦ機器２２４及び２２６を作動させる作動要求信号を、ＥＳＦＡＳ優先度論理２２０／２２２にそれぞれ送信する。

【０１１３】

図２Ａ～２Ｂ及び図３Ａ～３ＢにおけるＭＰＳ２００の図示された実装形態は、主要要素間の高いレベルの独立性を保証する。これは、センサ及び検出器の４つの分離グループ２０２ａ～２０２ｄ、（「ａ」～「ｄ」とラベル付けされる）トリップ決定の４つの分離グループ、ＲＴＳ２１４／２１４の２つの区分（述べた区分Ｉ及び区分ＩＩ）、ＥＳＦＡＳ回路構成２１２／２１８の２つの区分（述べた区分Ｉ及び区分ＩＩ）、及びＥＳＦ機器２２４／２２６の２つの区分（述べた区分Ｉ及び区分ＩＩ）の間の独立性を含む。（例えば、トリップ決定２０８ａ～２０８ｄ内の）ＳＦＭへの入力に基づいて、ＭＰＳ２００は、４つの分離グループの各々の中に安全機能のセットを独立に実装する。安全機能独立性は、センサ２０２ａ～２０２ｄからトリップ決定出力２１０ａ～２１０ｄまで維持される。この構成は、幾つかの局面では、ＳＦＭ故障を、そのモジュールの入力に基づくＳＦＭ故障に限定する。この戦略は、共通原因故障の影響を制限し、信号多様性を高めるのに役立ち得る。独立性のこの方法はまた、独立した安全機能内の故障が、他の安全機能モジュールのいずれかに伝搬しないことを保証し得る。更に、故障したＳＦＭのオンライン置換は、もしあれば他のモジュールに対する影響が最小の状態で故障が正される可能性があることを保証する。

【０１１４】

図示されたＭＰＳ２００内での安全機能データの通信は、３重モジュールで冗長性があり独立した光学式絶縁一方向通信経路によって送受信される。この通信スキームは、区分間投票を除いて、安全機能が、その安全機能を達成するため、その区分の外部に起因するあらゆる情報又はリソースにも依存しないことを保証し得る。クラス１Ｅ区分（例えば、区分Ｉ及びＩＩ）間の故障伝搬は、区分トリップ信号の一方向絶縁（例えば、光学式絶縁又はその他）によって防止される。

【０１１５】

図２Ａ～２Ｂ及び図３Ａ～３ＢにおけるＭＰＳ２００の図示された実装形態は、図示されたアーキテクチャの複数のエリアにおいて冗長性を更に組み込んでいる。ＭＰＳ２００内の冗長性は、（「ａ」～「ｄ」とラベル付けされる）センサ及び検出器の４つの分離グループ、（「ａ」～「ｄ」とラベル付けされる）トリップ決定、及びＲＴＳ及びＥＳＦＡＳ回路構成の２つの区分（述べた区分Ｉ及び区分ＩＩ）を含む。ＭＰＳ２００はまた、原子炉トリップ又はＥＳＦ機器作動が、必要されるときに起こることを、始動信号の単一の故障が妨げないように４分の２投票を用いる。更に、始動信号の単一の故障は、偽りの又は意図しない原理炉トリップ又はＥＳＦ機器作動が必要とされないときに、それらをもたらさないことになる。

【０１１６】

ＭＰＳ２００はまた、安全機能の各セットを実装することによって機能独立性を組み込み、安全機能の各セットは、独立したＳＦＭ上での特定の過渡事象を、安全機能のその特定のセットのための固有の論理エンジンによって緩和するのに使用される。

【０１１７】

幾つかの局面において、ＭＰＳ２００は、原子炉システムのために、簡単で信頼性が高く安全な設計を実現する設計技法を実装する。例えば、ＭＰＳ２００は、４つの分離グループ及び２つの区分の対称アーキテクチャに基づいてもよい。４つの分離グループの各々は、他の分離グループと機能的に同等であってもよく、２つの区分の各々は、機能的に同等であってもよい。上述したように、４分の２投票は、図示された実装形態において唯一の投票戦略であってもよい。別の例として、ＭＰＳ２００の論理は、特定の安全機能又は安全機能のグループに専用の有限状態機械（例えば、デジタル論理回路の集合体であって、有限数の状態のうちの１つの状態にある可能性があり、一度に、現在状態と称されるただ１つの状態にあるが、例えば状態遷移等のトリガー用の事象又は条件のセットによって始動されると１つの状態から別の状態に変化し得る、デジタル論理回路の集合体）に実装してもよい。そのため、カーネル又はオペレーティングシステムが全く必要とされない。別の例として、ＭＰＳ２００内の通信は、決定論的プロトコルに基づいてもよく、全ての安全データは、冗長性がある通信経路によって通信される。別の例として、ＭＰＳ２００の多様性属性は、完全に異なるプラットフォームに基づく更なるシステムの更なる複雑さなしで、アーチテクチャに固有であるように設計されてもよい。

【０１１８】

例えば、図４Ａ～４Ｂは、ＭＰＳ２００内に実装される多層化多様性戦略が、ソフトウェアベース又はソフトウェア論理ベース共通原因故障をどのように緩和するかを図示する例示的なチャート４００及び４５０をそれぞれ図示している。チャート４００及び４５０は、ＭＰＳ２００内に実装される多層化多様性戦略が、ＭＰＳ（例えばＭＰＳ２００）内のソフトウェアベース又はソフトウェア論理ベースＣＣＦについての懸念をどのように排除することができるかを図示している。これらの例において、過渡事象は、原子力システムのための給水の喪失である。図示されるように、２つの異なるプロセスパラメータＡ１及びＡ２が（例えば、センサ２０２ａ～２０２ｄを通して）測定される。Ａ１は、図示されるように温度パラメータである一方、Ａ２は、図示されるように、圧力である。

【０１１９】

異なるプロセス測定値Ａ１及びＡ２は、図示されるように、２つの異なる安全機能アルゴリズム、すなわち、（Ａ１）高温及び（Ａ２）高圧に入力される。２つの安全機能アルゴリズムの各々は、分離グループ内の別個でかつ独立したＳＦＭ上に位置する。安全機能アルゴリズムは、ＭＰＳ２００と共に示されるように、４つの分離グループ（Ａ，Ｂ，Ｃ，Ｄ）に分割されるプログラマブルデジタルハードウェアの２つの異なるセット（Ａ／Ｃ及びＢ／Ｄ）と、２つの区分とを使用して実装されてもよい。例えば、ここでは、２つの安全機能は、安全機能の単一のセットを備える。（例えば、２つの安全機能アルゴリズムの）各セットは、異なる技術に基づいてもよい。

【０１２０】

プログラマブルデジタルハードウェアの各セットは、設計ツールの異なるセットを使用して異なる設計チームによって設計され得るため、設計多様性もまたプロセスによって組み込まれる。一例として、安全機能は、マイクロプロセッサに実装されてもよい。この例において、安全機能は、シーケンシャルな方法で評価されてもよく、シーケンシャルな方法は、幾つかの局面において、処理ループのシーケンシャル動作に起因して、１つの安全機能（例えばＡ２）の別の安全機能（例えばＡ１）に対する依存性を導入してもよい。別の例として、安全機能は、状態ベースフィールドプログラマブルゲートアレイ（ＦＰＧＡ）に実装されてもよい。この例において、各安全機能は、全ての他の安全機能と独立に評価されてもよい。この後者の例は、別の安全機能に対する１つの安全機能の処理のあらゆる依存性を除去することによって独立性の増加を保証し得る。

【０１２１】

給水喪失の過渡事象の例についての多層化多様性は、ソフトウェアＣＣＦを特定の安全機能（Ａ１）の１つのセット（Ａ／Ｃ）に限定することによって、保護動作を無効化するＣＣＦに対する保護を提供する。幾つかの局面において、ソフトウェアＣＣＦは、２つの安全機能間の機能的独立性、及び、安全機能アルゴリズムが入力として使用するプロセス

測定値に基づいて特定の安全機能に限定される。幾つかの局面において、ソフトウェアＣＣＦは、各セットについて異なるプログラマブルハードウェア、設計チーム、及び設計ツールを組み込むことによって、特定の安全機能の１つのセットに限定される。ＣＣＦが特定の安全機能の１つのセットに限定された状態で、過渡事象は、その安全機能（Ａ１）の他のセット（Ｂ／Ｄ）又は第２の安全機能（Ａ２）の双方のセット（Ａ／Ｃ及びＢ／Ｄ）によって緩和される。

【０１２２】

例えば、図４Ａに示されるように、保護動作が（例えばチェックマークで示される）４つ全ての分離グループ（Ａ，Ｂ，Ｃ，Ｄ）によってとられる必要があることを示すＡ１についての安全機能の出力は、（例えば、「トリップ）」で示される）保護動作の始動をもたらす。図４Ｂに示されるように、安全機能Ａ１について、２つの分離グループ（Ａ及びＣ）、更に単一の区分内の２つのグループ内にＣＣＦが存在する場合、他の分離グループ（Ｂ及びＤ）内の保護動作の肯定的な指示は、（上述した４分の２スキームにおいて）保護動作を始動するのに十分な投票を依然としてもたらす。更に、安全機能Ａ１についてのグループＡ及びＣ内のＣＣＦは、各ＳＦＭに関する評価が独立しているため、安全機能Ａ２に伝搬しない。

【０１２３】

図５は、原子力システムのためのＩ＆ＣシステムのＭＰＳの安全機能モジュール（ＳＦＭ）５００のブロック図を図示している。図６は、原子力システムのためのＩ＆ＣシステムのＭＰＳの通信モジュール（ＣＭ）６００のブロック図を図示している。図７は、原子力システムのためのＩ＆ＣシステムのＭＰＳの機器インタフェースモジュール（ＥＩＭ）７００のブロック図を図示している。（以下で論じる）図８は、筐体（例えば、１つ又は複数のＳＦＭ５００、ＣＭ６００、及びＥＩＭ７００を相互接続する機械的構造）内の通信経路を図示している。一般的に、（筐体８００によって図示され、以下で述べられる）筐体内で相互接続された図示されたモジュール５００、６００、及び７００は、ＭＰＳ２００の安全機能を実装し、分離グループレベルモジュール（例えば、信号調節器２０４ａ～２０４ｄ、トリップ決定２０８ａ～２０８ｄ）、ＲＴＳレベルモジュール（例えば、ＲＴＳ投票２１４／２１６）、及びＥＳＦＡＳレベルモジュール（例えば、ＥＳＦＡＳ投票２１２／２１８）を構成する。幾つかの局面において、３つの型のモジュール（５００、６００、及び７００）を有することは、作業ラインで交換可能なユニットの数を最小にし、それにより、旧式化を最小にすることができる。更に、これらのモジュール（５００、６００、及び７００）は、どの個々のモジュール（５００、６００、及び７００）における単一の故障も、他のモジュール又は他の安全機能に伝搬しないように機能的に独立であってもよい。更に、図８Ａ～８Ｃにおいて実装されるモジュール（５００、６００、及び７００）の組合せは、離散的で決定論的な安全信号経路をもたらし得る。

【０１２４】

幾つかの局面において、モジュール（５００、６００、及び７００）は、それらの機能的独立性を少なくとも部分的に規定する１つ又は複数の特性を有してもよい。例えば、モジュールの各々は、全体システム／アーキテクチャにおいて（例えば、ＭＰＳ２００において）各々の他のモジュールに対して完全に自律的であってもよい。別の例として、モジュールの各々は、全体システム／アーキテクチャにおいて各々の他のモジュールに対して自律的に、特定の意図された安全機能を実行してもよい。更に別の例として、モジュールの各々は、モジュールの特定の意図された安全機能に固有である専用論理を含んでもよい。したがって、機能的に独立した各モジュールは、特定の意図された安全機能を遂行するため、任意の他のモジュールからの論理又は機能に依存していなくてもよい。

【０１２５】

図５を見ると、ＳＦＭ５００は、図示されるように、センサ入力又は他のＳＦＭからのデータを処理して、特定のＳＦＭが割り当てられる分離グループ（例えば、分離グループＡ、Ｂ、Ｃ、又はＤ）について原子炉トリップ及び／又はＥＳＦ作動決定を行う。ＳＦＭ５００は、２つの別個の構成、すなわち、（１）安全データバス通信によるセンサ信号調

節及び原子炉トリップ及び／又はＥＦＳ作動、並びに、（２）原子炉トリップ決定及び／又はＥＦＳ作動決定を伴う安全データバス通信において使用され得る。

【０１２６】

図示されるように、ＳＦＭ５００は、一般的に、入力ブロック５０４、機能論理ブロック５１２、並びに通信ブロック５１４、５１６、及び５１８を含む。（図５には４つが示される）各入力ブロック５０４は、信号調節回路５０６、アナログ・デジタル（Ａ／Ｄ）変換器５０８、及びシリアルインタフェース５１０からなる。各入力ブロック５０４は、（例えば、センサ２０２ａ～２０２ｄと同じか又は類似し得る）センサ５０２に通信可能に接続される。示されるように、個々のＳＦＭ５００は、（図示された例示的な実施形態において）最大４つの入力ブロック５０４を扱うことができる。入力型は、許可及びインターロックの生成を含む、トリップ又はＥＳＦ作動決定を行うためにＳＦＭ５００が必要になるであろうアナログ及びデジタル（例えば、４～２０ｍＡ、１０～５０ｍＡ、０～１０Ｖ）の任意の組合せであってもよい。

【０１２７】

機能論理ブロック５１２は、（使用される場合）入力ブロック５０４のシリアルインタフェース５１０からの出力を工学的単位に変換するＳＦＭ５００のプログラマブル部分である。機能論理ブロック５１２はまた、（例えば、センサ５０２からのセンサ測定値に基づく）入力ブロック５０４の出力及び／又は安全データバスからの情報に基づいてトリップ及び／又はＥＳＦ作動決定を行ってもよい。機能論理ブロック５１２はまた、許可を生成し、インターロックを制御してもよい。図示されるように、機能論理ブロック５１２は、複数の決定論的論理エンジンからなり、決定論的論理エンジンは、入力ブロック５０４及び／又は安全データバスから得られる情報を利用して、トリップ又はＥＳＦ作動決定を行う。

【０１２８】

機能論理ブロック５１２によって利用される設定点及び他の調整可能情報は、（例えば、ＳＦＭ５００上の）不揮発性メモリに格納され得る。これは、基礎にある論理を修正することなく、変更を可能にし得る。更に、機能多様性、信号多様性、及びソフトウェア多様性を実装するため、ＡＯＯ又はＰＡを緩和するのに使用される主要機能及びバックアップ機能は、同じＳＦＭ５００上にはなくてもよい。そのため、機能又は機能のグループのための専用ＳＦＭ５００を使用することによって、また、主要機能及びバックアップ機能が別個のモジュール５００上にあることを保証することによって、ソフトウェアＣＣＦの影響は、各モジュール５００上の論理及びアルゴリズムが固有であることに起因して制限される。

【０１２９】

通信ブロック５１４／５１６／５１８は、５つの別個の通信ポート（例えば、５１４とラベル付けされた３つの安全データポート、５１６とラベル付けされた１つのポート、及び５１８とラベル付けされた１つのポート）からなる。各ポートは、機能的に独立であり、監視及び指示（Ｍ／Ｉ）バス（例えば、ブロック５１６）、メンテナンスワークステーション（ＭＷＳ）バス（例えば、ブロック５１８）、又は安全バス（例えば、ブロック５１４）のいずれかとして指定される。各安全データバス５１４は同じデータを通信してよいものの、各通信ポートは、非同期であり、ポートは、独立しかつ固有の異なる通信エンジンを使用することによって異なるようにデータをパッケージし送信する。例えば、１つの安全データバス５１４は、例えば、シーケンシャルな順序（例えば、１、２、…、１０）でデータの１０パケットを送信してもよい一方、別の安全バス５１４は、同じ１０パケットを逆順（例えば、１０、９、…、１）で送信し、第３の安全バス５１４は、最初に偶数パケットを、それに続いて奇数パケットを送信する（例えば、２、４、…、１０、１、３、…、９）。この３重モジュール冗長性及び多様性は、通信エラー検出を可能にするだけでなく、ＲＴＳ又はＥＳＦＡＳが正しいトリップ及び／又は作動決定を行う能力に影響を及ぼすことなく、通信ＣＣＦを特定のバスに限定する。

【０１３０】

図６を見ると、ＣＭ６００は、原子力システム（例えば、ＭＰＳ２００）のためのＩ＆ＣシステムのＭＰＳの分離グループレベル相互接続、ＲＴＳレベル相互接続、及びＥＳＦＡＳレベル相互接続内で、例えばＳＦＭ５００及びＥＩＭ７００等のＭＰＳの他のモジュール間の独立しかつ冗長性がある通信を提供する。例えば、ＣＭ６００は、データがＭＰＳ内で通過するパイプライン並びにデータのこうした通過のスケジューラであってもよい。ＣＭ６００は、任意の特定のチャネルにおいて、そのチャネル内でのデータの操作／通過を制御してもよい。ＣＭ６００の図示された実装形態において、３つの型のブロック、すなわち、制限付き通信ブロック（ＲＣＢ）６０４、通信スケジューラ６０６、及び通信ブロック６０８／６１０が存在する。

【０１３１】

ＲＣＢ６０４は、図示されるように、４つの通信ポートからなる。幾つかの局面において、各ポートは、異なる一方向（例えば、受信のみ又は送信のみ）経路になるよう構成され得る。幾つかの実装形態において、図示されたＣＭ６００の場合と同様に、特定のＲＣＢ６０４から受信又は送信される情報は、光絶縁器６０２を通過する。幾つかの事例において、光絶縁器６０２は、任意の特定のトリップ決定からのデータが他のトリップ決定のデータから絶縁され、それにより、独立した冗長性を確保することを保証するのに役立ち得る。

【０１３２】

通信スケジューラ６０６は、通信ブロック６０８／６１０からＲＣＢ６０４に、又は、ＲＣＢ６０４から通信ブロック６０８／６１０にデータを移動させることを担う。幾つかの局面において、通信エンジン６０６は、例えばＦＰＧＡ等のプログラマブル論理、マイクロプロセッサ、又は述べた相互接続の間で通信をスケジュールするようにプログラムされる他の離散的論理からなる。

【０１３３】

通信ブロック６０８／６１０は、４つの別個の通信ポート（例えば、６０８とラベル付けされた３つの安全データポート及び６１０とラベル付けされた１つのポート）からなる。各ポートは、機能的に独立であってもよく、監視及び指示（Ｍ／Ｉ）バス（例えば、ブロック６１０）又は安全データバス（例えば、ブロック６０８）として指定される。幾つかの局面において、Ｍ／Ｉバス６１０は、ＭＰＳ（例えば、モジュール５００、６００、及び７００）内の全てのモジュールから、こうしたモジュールの各々の状態を含む情報を収集してもよく、その情報を「ヒストリアン」ステーション（例えば、ＭＰＳの履歴データのための専用コンピューティングシステム）に送信する。

【０１３４】

各安全データバス６０８は同じデータを通信してもよいものの、各通信ポートは、バス５１４を参照して上述したように、データを異なるようにパッケージし送信する。通信モジュールのアプリケーションに応じて、４つの通信ブロック６０８／６１０は、一方向及び２方向経路の任意の組合せで構成され得る。

【０１３５】

図７を見ると、ＥＩＭ７００は、一般的に、ＲＴＳ及び／又はＥＳＦＡＳレベルシステム内の原子力システム内で各コンポーネントに対するインタフェースを提供して、トリップ決定が投票され、コンポーネントレベルの作動及び操作が行われる。図示されるように、ＥＩＭ７００は、出力ブロック７２０、機器フィードバックブロック７１８、１Ｅ手動入力７１６、非１Ｅ手動入力７１４、投票エンジン７２２、優先度論理ブロック７２１、機器制御ブロック７２３、及び通信ブロック７２４／７２６／７２８を含む。一般的に、ＥＩＭ７００は、トリップ信号に基づいて、投票また幾つかの場合には２重投票（例えば、通信のための３分の２投票及びトリップ信号のための４分の２投票）を実行して、単一のコンポーネントの故障が、原子力システム（例えば、ＭＰＳ２００）のためのＩ＆ＣシステムのＭＰＳのチャネルレベル相互接続、ＲＴＳレベル相互接続、及びＥＳＦＡＳレベル相互接続内で伝搬しないことを保証してもよい。ＥＩＭ７００は、投票７２２、手動作動／１Ｅ入力７１６、及び非１Ｅ入力７１４からの自動信号について優先度割当てを実行

してもよい。
【０１３６】
出力ブロック７２０は、図示されるように、外部回路内で使用される可能性があり、かつ、電気負荷７０２（例えば、アクチュエータ）に接続される、最大３つの独立した出力スイッチ、又は幾つかの例ではそれより多い出力スイッチを含む。幾つかの局面では、これにより、ＥＩＭ７００は、単一のコンポーネントを直接制御するか又は複数のコンポーネントのための始動信号を提供できる。例えば、出力ブロック７２０はリレーを励磁し、リレーは種々のポンプを始動させ、複数の弁を開放する。各出力ブロック７２０はまた、自己試験し、負荷連続性チェックを実行する能力を含んでもよい。
【０１３７】
機器フィードバックブロック７１８は、示されるように、機器からの複数の（例えば、最大３つ又は幾つかの例ではそれより多い数の）フィードバック入力７０４からなってもよい。フィードバック入力７０４は、例えば、弁位置（例えば、完全に開放、完全に閉鎖）、遮断器状態（例えば、閉鎖／開放）、又は他のコンポーネントからの他のフィードバックを含み得る。機器フィードバック７０４は、以下で論じるように投票機器制御ブロック７２３内で使用され得る。
【０１３８】
１Ｅ手動入力ブロック７１６は、複数の（例えば、最大２つ又は幾つかの例ではそれより多い数の）手動入力信号７０６を提供してもよい。ＥＩＭ７００のこの部分は、手動入力に専用であってもよく、優先度論理ブロック７２１において利用される。
【０１３９】
複数の入力信号７０８は、絶縁インタフェース７１２を介して非１Ｅ入力ブロック７１４に接続される。この電気的絶縁インタフェース７１２は、優先度論理ブロック７２１への入力について非１Ｅ信号の使用を可能にする。
【０１４０】
投票エンジン７２２は、通信ブロック７２４からトリップ決定入力を受信する。投票の結果は、自動作動信号のために作動又は非作動信号を優先度論理ブロック７２１に提供する。幾つかの局面において、投票エンジン７２２は、投票スキームまた幾つかの場合には２重投票スキームを実装して、ＭＰＳ内の単一のコンポーネントの故障が伝搬しないことを保証してもよい。例えば、幾つかの局面において、投票エンジン７２２は、通信ブロック７２４においてトリップ決定を受信する。各通信ブロック７２４は、４つのチャネル又は分離グループ（例えば、上述したチャネルＡ～Ｄ）からトリップ決定（例えば、トリップ又はトリップなし）を受信してもよい。投票エンジン７２２内では、幾つかの局面において、３つの「Ａ」トリップ決定、３つの「Ｂ」トリップ決定、３つの「Ｃ」トリップ決定、及び３つの「Ｄ」トリップ決定が存在してもよい。そのため、投票エンジン７２２は、４つのチャネル又は分離グループの各々に関して３分の２決定を実行してもよい。例えば、３つの「Ａ」チャネルのうちの少なくとも２つがトリップの有効通信（例えば、トリップ決定の通信が有効であることを示す）を提供する場合、投票エンジン７２２は、少なくとも最初に、チャンル「Ａ」上にトリップが存在することを通信してもよい一方、３つの「Ａ」チャネルのうちの１つだけがトリップを示す場合、投票エンジン７２２は、チャネル「Ａ」上にトリップが存在しないと判定してもよい。
【０１４１】
投票エンジン７２２は、先に述べたように、２重投票スキームを実装して、ＭＰＳ構造全体にわたって故障が伝搬しないことを更に保証してもよい。例えば、上述した３分の２通信決定に続いて、投票エンジン７２２はまた、（例えば、偽りのトリップを示す故障と対照的に）トリップが実際に起こったのかを判定するために、４分の２トリップ決定を実行してもよい。例えば、３つの決定のうちの２つを実行する投票エンジン７２２内の４つの投票ブロック（例えば、３つの投票論理ゲートのうちの２つ）の出力を、４つの決定のうちの２つを行う別の投票ブロック（例えば、４つの投票論理ゲートのうちの２つ）に送ってもよい。第１の階層投票ブロック（例えば、３つのブロックのうちの２つ）からの４

つの出力のうちの少なくとも２つがトリップを示す場合、投票エンジン７２２は、トリップが起こった、（また、例えば負荷７０２等のＥＦＳ機器が作動されるべきである）と判定してもよく、そうでなければ、投票エンジン７２２は、実際にはトリップが全く起こらなかったと判定してもよい。

【０１４２】

優先度論理ブロックは、投票ブロック７２２、１Ｅ手動入力ブロック７１６、及び非１Ｅ手動入力ブロック７１４から入力を受信する。優先度論理ブロック７２１は、その後、全ての入力に基づいて、何を実行するよう機器制御モジュールに指令するかを決定する。

【０１４３】

機器制御ブロックは、優先度論理モジュールからコマンドを受信し、出力ブロック７２０を介してコンポーネントに対して適切な作動又は操作を実行する。機器制御ブロックは、機器制御目的のために、機器フィードバックブロック７１８を介して機器からフィードバックを受信する。

【０１４４】

機器制御ブロック７２２、優先度論理ブロック７２１、及び投票ブロック７２２はそれぞれ、状態情報をメンテナンスワークステーション（ＭＷＳ）バス（例えば、ブロック７２８）に提供する。通信ブロック７２４／７２６／７２８は、５つの別個の通信ポート（例えば、７２４とラベル付けされた３つの安全データポート、７２６とラベル付けされた１つのポート、及び７２８とラベル付けされた１つのポート）からなる。各ポートは、機能的に独立であってもよく、監視及び指示（Ｍ／Ｉ）バス（例えば、ブロック７２６）、メンテナンスワークステーション（ＭＷＳ）バス（例えば、ブロック７２８）、又は安全データバス（例えば、ブロック７２４）のいずれかとして指定される。

【０１４５】

図８は、１つ又は複数のＳＦＭ５００、ＥＩＭ７００、及びＣＭ６００を通信可能に接続する原子炉保護システム（例えば、ＭＰＳ１４５）の筐体８００の例示的な実施形態を図示している。この図は、筐体８００内で４つのＣＭ６００に接続された３つのＳＦＭ５００又はＥＩＭ７００の例を提示する。この例において、５つのデータバス経路が示されている。例えば、Ｘ、Ｙ、及びＺとそれぞれラベル付けされた３つの安全データポート８０２が存在する。Ｍ／Ｉとラベル付けされた１つのデータバス経路８０４が存在する。ＭＷＳとラベル付けされた１つのデータバス経路８０４が存在する。各データバス経路８０２／８０４は、この例において、筐体８００内で全ての他のデータバス経路８０２／８０４から機能的にかつ電気的に独立であってもよい。

【０１４６】

この図示された実施形態において、ＣＭ６００の各々は、データバス経路８０２／８０４のうちの１つのマスターを含んでもよい。図示されるように、Ｘデータバス経路８０２のマスター８０８は、安全データＸのためのＣＭ６００の一部である。Ｙデータ経路８０２のマスター８１０は、安全データＹのためのＣＭ６００である。Ｚデータ経路８０２のマスター８１２は、安全データＺのためのＣＭ６００である。最後に、この例に示すように、Ｍ／Ｉデータ経路８０４のためのマスター８１４は、Ｍ／ＩのためのＣＭ６００である。同様にこの例において、（例えば、メンテナンスワークステーションとして）別々に接続される、ＭＷＳデータ経路８０６のマスターであるＭＷＳマスター８１６が存在する。メンテナンスワークステーション（ＭＷＳマスター）８１６は、配線スイッチによって、機器の正常運転のために切り離されてもよい。

【０１４７】

図９Ａ～９Ｃは、ＳＦＭ５００、ＣＭ６００、及びＥＩＭ７００の１つ又は複数を利用する分離グループレベル相互接続、ＲＴＳレベル相互接続、及びＥＳＡＦＡＳレベル相互接続のブロック図を図示している。一般的に、モジュールＳＦＭ５００、ＣＭ６００、及びＥＩＭ７００は、例えば、隣接するか又は他の安全機能に単一の故障（例えば、ハードウェア、ソフトウェア、又はその他）が伝搬することに対する保護をもたらす機能的に独立したモジュール（例えば、相互接続されたコンポーネントのアセンブリであって、識別

可能なデバイス、計器、又は機器要素を構成し、切り離すことができ、ユニットとして除去することができ、またスペアと置換することができ、そのアセンブリがユニットとして試験されることを可能にする定義可能な性能特性を有する、アセンブリ）として、ＭＰＳ２００内に配置され得る。モジュールは、トリップ検知及び決定のために、幾つかの実装形態において、最大３重冗長性を提供してもよい。モジュールは、同様に、上述したように、冗長性があるＲＴＳ及びＥＳＦＡＳ投票区分を提供するために配置されてもよい。幾つかの実装形態において、モジュールは、トリップコンポーネント（例えば、遮断器、センサ、又はその他）毎に複数の独立したトリップ投票モジュールを提供してもよい。

【０１４８】

幾つかの場合において、モジュールはＲＴＳ投票を提供する一方、他の場合において、モジュールはＥＳＦＡＳ投票を提供する。各モジュールの独立性に関して、各モジュールは、特定のトリップコンポーネントに専用の全ての他のモジュールとは別に、特定のトリップについて決定を行って、ＲＴＳ／ＥＳＦＡＳトリップを起動しても又は起動しなくてもよい。幾つかの実装形態において、トリップ決定の有効通信の決定は、多数（例えば、３分の２）によって行ってもよい。幾つかの実装形態において、決定は、２重投票スキームにおいて行なわれてもよく、２重投票スキームにおいて、トリップ決定の通信は多数決（例えば、３分の２）によって有効化され、２次トリップ決定投票は、多数に満たない（例えば、４分の２）投票による。

【０１４９】

図９Ａを見ると、例示的な分離グループレベル相互接続９００が図示されている。図示されたチャネルレベル相互接続９００は、チャネルセンサ入力９０２、入力９０２を受信するＳＦＭ５００、及び９２０を通して出力９０４を通信するＣＭ６００を含む。示されるように、単一の機能又は機能の単一のセットを実装するため、チャネルレベル相互接続９００における各ＳＦＭ５００は、アナログ及びデジタルの任意の組合せで、４つの入力９０２又は幾つかの事例ではそれより多い入力９０２を含み得る。各入力９０２は、特定のＳＦＭ５００に固有であってもよい（例えば、チャネルＡ加圧器圧力信号は、１つのＳＦＭ５００だけに対する直接入力である）。入力データは、状態情報（例えば、アラーム、論理決定、モジュール状態）と共に、４つ全てのデータバス上で利用可能であってもよい。

【０１５０】

安全バスは、機能的に独立であってもよく、各安全バスはマスター・スレーブプロトコルを使用し、マスターはＣＭ６００である。ＳＦＭ内のブロックは同期して運転するものの、モジュール間の通信は非同期であってもよい。或るバスのためのＣＭ６００が特定のＳＦＭ５００から情報を要求するとき、ＳＦＭ５００は、ブロードキャストによってバスに応答してもよい。ブロードキャストの利点は、例えば、「１」とラベル付けされるＳＦＭ５００が「２」とラベル付けされるＳＦＭ５００が必要とする情報（例えば、許可信号、センサ入力値）を有する場合、ＳＦＭ５００「２」は、傾聴し、必要とされる情報を取得することができるということである。

【０１５１】

（例えば、「Ｘ」、「Ｙ」、及び「Ｚ」とラベル付けされる）３つの安全データバスに加えて、監視及び指示（Ｍ／Ｉ）のための第４の図示された通信バスが存在する。Ｍ／Ｉバスのマスターは、Ｍ／Ｉデータを安全ゲートウェイ及び非安全制御システムに提供することに専用のＣＭ６００であってもよい。３つの安全データバス（例えば、バスＸ、Ｙ、及びＺ）のためのＣＭ６００とは違い、Ｍ／Ｉ　ＣＭ６００は、３つの全ての安全バス上のブロードキャスト情報を傾聴できてもよい。

【０１５２】

幾つかの実装形態において、ＣＭ６００の制限付き通信ブロック（ＲＣＢ）は種々のポイント・ツー・ポイント構成を有し得る。分離グループレベル相互接続９００において、ＲＣＢ上の４つの全ての通信ポートを、送信だけのために構成してもよい。各安全データバスＣＭ６００（例えば、Ｘ、Ｙ、及びＺとラベル付けされるＣＭ６００）からのデータ

を、ＲＴＳ及びＥＳＦＡＳの各区分（例えば、区分Ｉ及びＩＩ）に送信してもよい。Ｍ／Ｉ　ＣＭ６００からのデータ（例えば、出力９１６～９２０）を、安全ゲートウェイ及び非安全制御システムに送信してもよい。

【０１５３】

出力９０４～９１４を、例えば、ＲＴＳレベル相互接続及びＥＳＦＡＳレベル相互接続に提供してもよい（以下で述べる）。例えば、図示されるように、出力９０４、９０８、及び９１２を、ＥＳＦＡＳレベル相互接続に提供してもよい一方、出力９０６、９１０、及び９１４を、ＲＴＳレベル相互接続に提供してもよい。１つだけの分離グループレベル相互接続９００が図９Ａに示されているものの、ＭＰＳ構造内に複数の相互接続９００が存在してもよい。

【０１５４】

図９Ｂを見ると、区分によって分割された例示的なＲＴＳレベル相互接続が示されている。ＲＴＳレベル相互接続は、示されるように、ＲＴＳの区分Ｉ及びＩＩ（例えば、ＲＴＳ投票２１４及び２１６）を含む。図示された各区分（２１４及び２１６）は、４つのＣＭ６００及び４つのＥＩＭ７００を含む。各区分について、（Ｘ、Ｙ、及びＺとラベル付けされる）３つの安全データバスの各々は、（例えば、同じ数値、すなわち、Ａ１及びＢ１でラベル付けされる分離グループを有する）入力９６２～９７２として示されるトリップ又はトリップなし決定を４つの全ての分離グループから受信してもよい。第４のＣＭ６００を、示されるように、非安全制御システム及び安全ゲートウェイに（出力９７４～９７６として）データを送信するために設けてもよい。

【０１５５】

各安全バスＣＭ６００のためのＲＣＢ上の各通信ポートを、「受信のみ」のために構成してもよく、また、（上述したように）光学的に絶縁してもよい。Ｍ／Ｉ　ＣＭ６００は、「送信のみ」のために構成されたＲＣＢにおける全てのポートを有してもよい。

【０１５６】

幾つかの実装形態において、全ての分離グループからの各安全データバスについてのトリップ決定は、４つのＥＩＭ７００の各々に利用可能である。ＥＩＭ７００は、（Ｘ、Ｙ、及びＺとラベル付けされる）３つ全ての安全バスを使用して、通信エラーに起因する遮断器の誤った作動が全く存在しないことを保証してもよい。４つの分離グループ（入力９６２～９７２）のうちの少なくとも２つがトリップ状態を示すとき、原子炉トリップ遮断器は開放される。各ＥＩＭ７００は、例えば、原子炉トリップ遮断器の不足電圧リレー及びシャントトリップコイルに専用であってもよい。自動作動に加えて、ＥＩＭ６００は、手動区分レベル原子炉トリップ９７８、遮断器フィードバック、及びＥＳＦＡＳフィードバックのための入力を有することになる。

【０１５７】

（区分Ｉの場合、９８０ａ～９８０ｄとラベル付けされ、区分ＩＩの場合、９８２ａ～９８２ｄとラベル付けされる）ＥＩＭ６００出力は、特定の区分に関連する（図２Ｂに示された）原子炉トリップ遮断器（ＲＴＢ）についてトリップコイルのための入力に接続されてもよい。

【０１５８】

図９Ｃを見ると、区分によって分割された例示的なＥＳＦＡＳレベル相互接続が示されている。ＥＳＦＡＳレベル相互接続は、示されるように、ＥＳＦＡＳの区分Ｉ及びＩＩ（例えば、ＥＳＦＡＳ投票２１２及び２１８）を含む。図示された各区分（２１２及び２１８）は、４つのＣＭ６００及び４つのＥＩＭ７００を含む。各区分について、（Ｘ、Ｙ、及びＺとラベル付けされる）３つの安全データバスの各々は、入力９６２～９７２としてラベル付けされるＥＳＦ作動決定を全ての分離グループ（この例では、Ｄとラベル付けされる４つの分離グループ）から受信する。

【０１５９】

（Ｘ、Ｙ、及びＺとラベル付けされる）各安全データバスＣＭ６００のためのＲＣＢにおける各通信ポートを、「受信のみ」のために構成し、また、（上述したように）光学的

に絶縁してもよい。Ｍ／Ｉ　ＣＭ６００は、「送信のみ」のために構成されるＲＣＢにおける全てのポートを有し、また、光学的に絶縁されてもよい。

【０１６０】

幾つかの実装形態において、全ての分離グループからのＥＳＦ作動決定は、（Ｘ、Ｙ、及びＺとラベル付けされる）３つの全ての安全データバス上のＥＩＭ７００に利用可能である。例えば、ＥＩＭ７００は、３つの全ての安全データバスを使用して、通信エラーによって引き起こされる機器の誤作動が全く存在しないことを保証してもよい。（例えば、入力９６２～９７２上で）４つの分離グループのうちの少なくとも２つがＥＳＦ作動についての必要性を示すとき、安全機能を、（図３Ｂに示すように、区分に基づいてＥＳＦ機器２２４及び２２６に接続される）出力９９０を通して始動してもよい。幾つかの局面において、各ＥＩＭ７００は、個々のコンポーネント（例えば、単一のＥＳＦコンポーネント）に専用となり得る。

【０１６１】

自動始動以外に、各ＥＩＭ７００は、手動入力９９２を使用して、コンポーネントを制御できる。更に、各ＥＩＭ７００はまた、非１Ｅ制御入力９９４を受信してもよい。（図３Ｂにおいて入力２８２としても示される）非１Ｅ制御入力９９４は、非１ＥのためのＥＩＭ７００に提供されて、ＥＩＭの出力に基づいて１Ｅ安全ＥＳＦコンポーネントを制御してもよい。コンポーネントフィードバック（例えば、リミットスイッチ）、投票決定、及び他の利用可能な情報（例えば、アラーム）は、出力９７４～９７６としてＭ／Ｉ　ＣＭ６００から送信されてもよい。

【０１６２】

図１０は、原子力システムのためのＩ＆Ｃシステム１３５のための多様性分析図を図示している。多様性分析の目的ために、図１０において特定されるブロックは、システム検査を簡略化する或るレベルの詳細を示す。ブロックは、機器及びソフトウェアであって、それらの内部故障がそれらの属性に基づいて他のブロックに伝搬しないと仮定され得る、機器及びソフトウェアの物理的サブセットを表すように選択された。

【０１６３】

図示されるように、図１０の図内のブロックは、Ｉ＆Ｃシステム、この例では、Ｉ＆Ｃシステム１３５を図示している。ブロック１００２は、非１Ｅ監視及び指示機器を表し、ブロック１００４ａ／ｂは、１Ｅ監視及び指示Ｉ及びＩＩをそれぞれ表し、ブロック１００６ａ／ｂは、安全ブロックＩ及びＩＩをそれぞれ表す。ブロック１００６ａは、分離グループＡ及びＣ、ＲＴＳ　Ｉ、及びＥＳＦＡＳ　Ｉを含む一方、ブロック１００６ｂは、分離グループＢ及びＤ、ＲＴＳ　ＩＩ、及びＥＳＦＡＳ　ＩＩを含む。ブロック１００８はＭＣＳを表す。図示されるように、矢印を有する接続ラインはブロック間の通信を示す。

【０１６４】

４つの階層についての目的のうちの１つは多様性である。例えば、ＭＰＳは、単一の故障基準を満たしてもよく、単一の故障基準は、（１）特定可能であるが検出可能でない全ての故障と同時発生の安全システム内の任意の単一の検出可能故障、（２）単一の故障によってもたらされる全ての故障、及び（３）安全機能を必要とする設計基準事象をもたらすか又は設計基準事象によってもたらされる全ての故障及び誤ったシステム動作の存在下で、設計基準事象について必要とされる全ての安全機能をＭＰＳが実行することを要求してもよい。この要件は、信頼性の増加を提供し得るが、システムが共通原因故障（ＣＣＦ）に脆弱であることを排除しない。任意の設計について、ＣＣＦを複数の独立した故障から区別する依存性（例えば、結合因子）が存在し得る。これは、システム内の共通原因故障を防止する２つの基本形態をもたらす、すなわち、原因となる影響が減少するか、又は、これらの影響に抗するシステムの能力が増加する。

【０１６５】

これらの２つの形態の実装形態は、上述した６つの属性、すなわち、設計多様性、機器多様性、機能多様性、人間多様性、信号多様性、及びソフトウェア多様性で実装され得る

。これらの属性の適用は、図１０に図示される各ブロック並びに図１０に示されるブロック間の属性に関して検査される。
［ブロック内の属性］
先の図を参照して図示され、また同様に述べるように、分離グループＡ、Ｂ、Ｃ、及びＤ並びにＲＴＳ及びＥＳＦＡＳの２つの区分は、それらが基づくプログラマブル技術に従ってグループ化される。安全ブロックＩ及びＩＩは共に、モジュール保護システム（ＭＰＳ）（例えばＭＰＳ２００）を構成する。
【０１６６】
信号多様性に関して、所与の過渡事象の場合、少なくとも２つの安全機能が存在する可能性があり、それぞれの機能は、異なる物理効果（例えば、圧力、レベル、温度、中性子束）の被測定変数に基づく。１つの安全機能の喪失は、ブロックが保護動作についての必要性を特定することを妨げない。
【０１６７】
ソフトウェア多様性に関して、その入力に基づいて、各安全機能モジュール（ＳＦＭ５００）は、安全機能又は安全機能のグループに専用である。結果として、各ＳＦＭは、固有のアルゴリズム／論理を有する。各通信モジュール（ＣＭ６００）は、同じ情報のパケットを、ＣＭにおける各通信エンジン（６０８／６１０）が異なるアルゴリズムを有することを必要とし得る異なる順序で送信する。各機器インタフェースモジュール（ＥＩＭ７００）は、単一のコンポーネントに専用であってもよく、固有のアルゴリズム／論理をもたらしてもよい。
【０１６８】
１Ｅ監視及び指示は、ビデオ表示ユニット（ＶＤＵ）及び物理的スイッチの２つの区分を使用して達成されてもよい。１Ｅ監視及び指示（Ｍ／Ｉ）の各区分はブロック１００４ａ／ｂであってもよい。設計多様性に関して、Ｍ／Ｉの各区分は、ディジタル表示上のプラント状態情報をオペレータに提供してもよく、また、区分レベルで、任意の保護動作を手動で始動する手動スイッチを有する。信号多様性に関して、オペレータは、ＭＰＳによって利用される全ての被測定変数を有し、トリップ及び／又はＥＦＳ作動が必要とされるかを判定してもよい。同程度に速くはないものの、オペレータは、異なる物理効果の複数の被測定変数を有して、ＭＰＳと同じ判定を行い得る。
［ブロック間の多様性属性］
人間多様性に関して、安全ブロックＩ及び１Ｅ　Ｍ／Ｉ　Ｉのソフトウェアは、１つの設計チームによって設計されてもよく、安全ブロックＩＩ及び１Ｅ　Ｍ／Ｉ　ＩＩは、異なる設計チームによって設計されてもよい。更に、独立した検証及び妥当性確認チームが、各設計チームの作業を再検討して、設計の正しさを保証し得る。先に述べた設計チームは、同様に、モジュール制御システム（ＭＣＳ）及び非１Ｅ　Ｍ／Ｉに割り当てられる設計チームとは異なる。
【０１６９】
設計多様性は、同じか又は類似の問題を解決するために、ソフトウェアとハードウェアとの双方を含む異なるアプローチを使用することである。ＣＣＦの可能性及び結果を制限するため、安全ブロックＩ　１００４ａ及び１Ｅ　Ｍ／Ｉ　Ｉ　ブロック１００６ａは、安全ブロックＩＩ及び１Ｅ　Ｍ／Ｉ　ＩＩとは異なるプログラマブル技術を使用してもよい。ＭＣＳ及び非１Ｅ　Ｍ／Ｉもまた、異なるプログラマブル技術を有してもよい。以下で論じる他の属性と共に、異なるハードウェア設計は、異なる故障モードを有してもよく、ひいては、ＣＣＦが２つ以上のブロックに影響を及ぼす可能性を減少させてもよい。例えば、Ｍ／Ｉブロックを除いて、ブロックは、異なる部屋に物理的に分離されてもよい。これは、複数のコンポーネントがＣＣＦ事象に関わる状態を生成し得る結合因子を更に減少させることが意図されている。
【０１７０】
ソフトウェア多様性は、設計多様性のサブセットであり、また、同じ安全目標を達成するための、異なる主要職員を有する異なる開発グループによって設計され、実装される異

なるプログラムの使用を含んでもよい。先に論じた設計多様性に起因して、異なる設計チームは、異なる設計ツールを使用してもよく、ひいては、ツールは、同じ故障モードを導入しなくてもよい。

【０１７１】

機能多様性は、ブロック間で異なる目的及び機能を有することによって導入されてもよい。安全ブロックＩ及びＩＩはＭＰＳを形成する。これらのブロックは、運転限界を超えた場合に原子炉トリップを始動し、ＥＳＦを始動して、想定事故を緩和してもよい。Ｍ／Ｉブロックによって、オペレータが、安全システムと非安全システムとの双方を監視及び制御することが可能になり得る。オペレータは、プラントを運転限界内に維持するか又は必要な保護動作を始動することができる。ＭＣＳは、システムの自動制御を提供して、或る運転上の過渡変化を制限することを含む運転限界内にプラントを維持することを提供する。

【０１７２】

ブロック間において、機器を作動する自動及び手動手段並びに保護動作を有することによって、信号多様性を提供してもよい。ＭＣＳ及び非１Ｅ　Ｍ／Ｉは、機器レベルの制御を提供する一方、１Ｅ　Ｍ／Ｉブロックは、区分レベルの制御を提供する。

【０１７３】

機器多様性は、類似の安全機能を実行するための異なる機器の使用である。保護動作の始動は、スイッチを使用してオペレータ動作によって行われ得る、又は、安全ブロックＩ又はＩＩによって自動的に実行され得る。安全ブロックＩとＩＩとの間において、異なるプログラマブル技術を使用してもよく、その技術は、異なる内部サブコンポーネント及び異なる製造方法を必要としてもよい。

【０１７４】

４つの階層の別の分析指針はシステム故障の型である。型１故障は、防護の階層の間の相互作用による制御システムエラーによって始動されるプラント過渡変化について、保護動作をとることができない故障である。通常、これは、共通のセンサ又は信号源の故障に関連する。ＭＰＳによって監視されるプラントパラメータのうちの幾つかは、正常なプラント制御のためにＭＣＳに提供される。上述したように、１つの信号源を設ける代わりに、４つの全ての分離グループ並びにＥＳＦＡＳ及びＲＴＳの双方の区分は、絶縁された一方向通信を通して情報を提供する。これによって、ＭＣＳが、冗長性がありかつ独立したどの信号源を使用するかを選択する異なる方法（例えば、中央信号選択）を使用できるようになり得る。

【０１７５】

型２故障は、過渡変化を直接もたらさない場合があり、また、検出されない故障であるため、保護機器がプラント過渡変化に応答しない場合がある故障である。安全ブロックＩ及びＩＩの中及びＩとＩＩとの間の属性を使用すると、検出されない故障又はＣＣＦが２つ以上のブロックに影響を及ぼすことを防止するのに十分な多様性が存在し得る。保護動作を自動的に始動するために必要とされる２つのブロックのうちの１つだけによって、型２故障を、更なるシステムなしで、ＭＰＳ（安全ブロックＩ及びＩＩ）によって緩和してもよい。

【０１７６】

型３故障は、設計基準事象を検出するのに依存する１次センサが異常な読みを生成する故障である。信号多様性は、任意の過渡事象について、少なくとも２つの安全機能をそれぞれ異なる測定パラメータに基づいて提供することによって安全ブロック内に存在し得る。所与の安全機能についての４つの全ての分離グループのセンサが異常な読みを提供する場合、型３故障について２つの考えられる不都合なシナリオ、すなわち、１）限界を実際に超えたときにトリップ又はＥＳＦ作動が全く必要とされないことを異常な読みが示すこと、及び、２）限度を超えなくてもトリップ又はＥＳＦ作動が必要とされること（例えば、誤ったトリップ又はＥＳＦ作動）を異常な読みが示すことが存在し得る。第１のシナリオにおいて、安全ブロック内でＣＣＦと同時発生の型３故障は、必要な保護動作の始動を

妨げないことがある。先に述べたように、信号多様性は、別個の安全機能が過渡事象を緩和するために利用可能であることを可能にし得る。ＭＰＳ内のＣＣＦは、２つの安全ブロックの一方の安全ブロックに限定され、また、保護動作の始動を妨げるか又は誤った指示による始動を妨げると仮定される。例えば、先に論じたように、４分の２一致論理は、全てのトリップ及びＥＳＦ作動のために使用されてもよく、４分の２一致論理は、４つの分離グループのうちの２つが、影響を受けない安全ブロック上の影響を受けない安全機能について、トリップ又はＥＳＦ作動についての必要性を示し、実行される動作のオペレータに肯定的な指示を提供する。

【０１７７】

第２のシナリオにおいて、安全ブロック内でＣＣＦと同時発生の型３故障は、誤ったトリップまたはＥＳＦ作動をもたらし、そのとき、１Ｅ　Ｍ／Ｉブロックは、１つのブロックが肯定的であり、かつ１つのブロックが成功裡の作動の誤った指示であることを示すか、又は、１つのブロックが肯定的であり、かつ１つブロックが作動の指示を有していないことを示す。いずれの場合も、誤った作動を評価しそれを正すことは、オペレータを長く拘束する場合があるが、必要に応じてコンポーネントを再整列させる能力は、同じＣＣＦによって影響を受けないであろう１Ｅ制御装置及び非１Ｅ制御装置の双方によって提供される。

【０１７８】

別の分析指針は階層要件である。システム検査を簡略化する詳細レベルを表すブロックを提供するため、防護の４つの概念的な階層が、幾つかのブロックにおいて組み合わされる（例えば、ＲＴＳ及びＥＳＦＡＳ）だけでなく、別個のブロック（例えば、安全ブロックＩ及びＩＩ、１Ｅ　Ｍ／Ｉ　Ｉ及びＩＩ）に分割される。幾つかの局面において、分離グループ、ＲＴＳ、及びＥＳＦＡＳは、それらが基づくプログラマブル技術に従って安全ブロックにグループ化される。例えば、ＭＰＳのそれぞれの半分（例えば、４つの分離グループのうちの２つ、ＥＳＦＡＳの２つの区分のうちの１つ、及びＲＴＳの２つの区分のうちの１つ）又は１つの安全ブロックは、十分な多様性属性を有してもよい。異なる設計チーム（人間多様性）は、異なるプログラマブル技術（設計及び機器多様性）に基づいて異なるプログラマブルデジタルハードウェアを利用し、異なるプログラマブル技術は、異なる設計ツール（ソフトウェア多様性）の使用を必要とする。Ｍ／Ｉ階層は、同様に別個のブロックに分割されてもよい。１Ｅ　Ｍ／Ｉブロックは、分割されて、１Ｅ　Ｍ／Ｉブロックが安全ブロックと類似の多様性属性を有することを特定してもよい。選択されたブロックがどのようにして防護の４つの階層の中に入るかが図１１に図示され、図１１はダイアグラム１１００を示す。

【０１７９】

別の分析指針は評価方法である。選択されるブロックは、（以下で論じる）出力信号指針に従って分析されると、想定されることを必要とするあらゆる想定故障も、最も弊害をもたらす結果を生成するように、「ブラックボックス」として考慮されるべきである。幾つかの局面において、作動するシステムの故障は、特に、自動化安全システム内のＣＣＦに起因する状態を特定し、それに応答するために必要とされる時間を分析するとき、最悪の事態の故障ではない場合がある。ブロックは、ハードウェアＣＣＦ及びソフトウェアＣＣＦに基づいて評価されることになる。各ＣＣＦについて、ブロックは、最も弊害をもたらす結果を生じ得る３つの考えられる出力、すなわち、１）誤った指示を有する故障したままの状態か又は必要とされるときの動作がない、２）成功裡の作動の指示を伴う、機能の誤った始動、及び３）成功裡の作動の指示のない、機能の誤った始動を有すると評価され得る。安全ブロックのうちのいずれかの安全ブロック内のＥＩＭは、ソフトウェアＣＣＦに対して脆弱であると考慮されない場合がある。例えば、ＥＩＭは、単一のＥＳＦコンポーネント又は原子炉トリップ遮断器並びに手動制御及び自動制御を有するインタフェースに専用の優先度論理モジュールであってもよい。有限状態機械の使用は、全ての考えられる入力、デバイス状態、及び状態機械の出力を含む、機能の網羅的な試験を可能にし得る。その試験可能性、ＥＩＭ多様性属性、及び単一のコンポーネントに専用であることに

基づいて、ＥＩＭは、ソフトウェアベースの又はソフトウェア論理ベースのＣＣＦの考慮が必要とされないほどに十分に簡素であってもよい。

【０１８０】

別の分析指針はブロックの想定共通原因故障である。１Ｅ　Ｍ／Ｉブロックは、ビデオ表示ユニット（デジタルハードウェア）と手動制御装置（非デジタルハードウェア）との組合せを含む。ＶＤＵは、指示のためだけに設計されてもよく、機器を制御する能力を持たない。各１Ｅ　Ｍ／Ｉブロック１００４ａ／ｂ内の手動制御は、安全ブロックＩ又はＩＩによって自動的に実行される任意の保護動作を区分レベルで始動する能力をオペレータに提供する。指示及び手動制御が、幾つかの例において異なるハードウェア（例えば、デジタル対オープン／クローズ接点スイッチ）である状態で、ＣＣＦは、両方ではないが、一方又は他方に影響を及ぼすと仮定され得る。ソフトウェアＣＣＦとハードウェアＣＣＦの双方について、故障したままの状態は、１つの区分のオペレータ表示が、誤った安全運転状態又は１つの区分の手動スイッチの故障を示すことをもたらす。ＶＤＵは、制御能力をほとんど又は全く有していない場合があるため、誤った作動を提供しない場合がある。しかしながら、ソフトウェアＣＣＦの場合、ＶＤＵは、成功裡の作動の誤った指示を提供するか又は不正確なプラント状態を提供し、オペレータが誤った保護動作を始動することを要求する場合がある。

【０１８１】

ＥＩＭを除いて、安全ブロック内のモジュールは、ソフトウェアＣＣＦを有すると想定される。安全ブロック内の多様性属性に起因して、ソフトウェアＣＣＦは、ＳＦＭ上のＣＭ又は機能に限定され得る。ＳＦＭが適切なトリップ決定を行うことを妨げる安全ブロック内のソフトウェアＣＣＦは、そのブロック内の機器、信号、及びソフトウェア多様性によって緩和され得る。それぞれの過渡事象の場合、事象を緩和するために必要とされる１次安全機能及びバックアップ安全機能は、異なる物理効果の被測定パラメータに基づく異なる論理／アルゴリズムを使用して別個の安全機能上に実装され得る。３重のモジュール冗長性の実装形態を有し、かつ、各データバスが異なる方法で同じ情報を送信すると、ソフトウェアＣＣＦを有するＣＭは、保護動作を誤って始動しないか又は、保護動作の始動を妨げない場合がある。結果として、最も弊害をもたらすシナリオは、ＥＳＦＡＳ機能の誤った作動をもたらすＳＦＭ内のソフトウェアＣＣＦである可能性がある。

【０１８２】

安全ブロック内のハードウェアＣＣＦは、必要な保護動作を検出し始動するブロックの完全故障であると想定され得る。ＥＳＦ機能の誤った作動をもたらすハードウェアＣＣＦは、ソフトウェアＣＣＦに起因する誤った作動と同じ影響を及ぼす場合があり、ひいては、ハードウェアＣＣＦについてやはり考えられない場合がある。

【０１８３】

非１Ｅ　Ｍ／Ｉは、安全及び非安全機器のための制御装置を含む。非１ＥのためのＶＤＵは、１Ｅ　Ｍ／Ｉによって使用されるＶＤＵとは異なる。非１Ｅ　Ｍ／Ｉが、正常な日々の運転のために使用されるため、非１Ｅ　Ｍ／Ｉサブシステム（例えば、タービン制御、給水制御）内のソフトウェア又はハードウェアＣＣＦによって誘起されるあらゆる誤った作動も即座に特定可能である場合があり、また、運転限界を超える場合、ＭＰＳ（安全ブロックＩ及びＩＩ）によって緩和される場合がある。非１Ｅについての想定故障は、１）成功裡の作動の指示がある、また、その指示がないサブシステムのコンポーネントの誤った作動を有する故障したままの状態、及び、２）どの機器も実際に作動されないときの成功裡の作動の指示を有する故障したままの状態である。

【０１８４】

ＭＣＳは、或る運転上の過渡変化を制限することを含む運転限界内に日々のプラント運転を維持するために依存する非安全システムを包含する。したがって、サブシステム（例えば、棒コントロール）のあらゆる故障も、オペレータによって即座に検出され得る。非１Ｅ　Ｍ／Ｉと同様に、ＭＣＳについての想定されるソフトウェア及びハードウェアＣＣＦは、１）成功裡の作動の指示がある、また、その指示がないサブシステムのコンポーネ

ントの誤った作動を有する故障したままの状態、及び、２）どの機器も実際に作動されないときの成功裡の作動の指示を提供する故障したままの状態をもたらす。

【０１８５】

別の分析指針は、同一のハードウェア及びソフトウェアモジュールの使用である。ここで、ブロック間の多様性は、同一であるブロックを考慮しないための基礎を提供する。これに基づいて、想定されるＣＣＦは、単一のブロックに限定され得る。

【０１８６】

別の分析指針は、他のブロックの影響である。全てのブロックは、正しい又は正しくない入力に応答して正しく機能すると仮定される。各ブロックは、独立し、別のブロック内の想定されるＣＣＦによって影響を受けないとみなされる。

【０１８７】

別の分析指針は出力信号である。幾つかの局面において、Ｉ＆Ｃアーキテクチャは、エラーが後方に伝搬して前のブロックの出力に入るのを防止し得る。安全ブロックＩ及びＩＩから１Ｅ　Ｍ／Ｉへの全ての情報は、（ＣＭ６００内に示される）光学的に絶縁された送信のみの通信エンジンを通して送出され得る。１Ｅ　Ｍ／Ｉから安全ブロックへの信号は、手動スイッチからのオープン／クローズ接点であってもよく、手動スイッチの位置又は接点状態を、安全ブロック内のＣＣＦは変更できない。安全ブロック間の通信情報は、分離グループＡ及びＣからＥＳＦＡＳ及びＲＴＳの区分ＩＩに、また、分離グループＢ及びＤからＥＳＦＡＳ及びＲＴＳの区分Ｉに送出されるデータであってもよい。４つの分離グループは、独立しかつ冗長性がある。しかしながら、図１０の例証のために、分離グループは、それらが使用するプログラマブル技術に従って安全ブロックにグループ化される。安全ブロックと１Ｅ　Ｍ／Ｉとの間の通信と同様に、分離グループからＲＴＳ及びＥＳＦＡＳの任意の区分への通信は、光学的に絶縁された送信のみの通信エンジンを通してもよい。安全ブロックへの非安全入力は、ＥＳＦＡＳ　ＥＩＭに対するものであってもよく、絶縁されたオープン／クローズ接点に限定されてもよい。

【０１８８】

安全ブロックからの全ての入力は、光学的に絶縁された送信のみの通信エンジンからであってもよい。これは、１Ｅ　Ｍ／Ｉ内のいずれのエラーも、後方に伝搬して安全ブロックに至ることを防止し得る。

【０１８９】

別の分析指針は、予測運転事象についての多様性である。過渡事象に関連する単一のＣＣＦ又は型２故障は、ＭＰＳがその安全機能を実行することを妨げない場合がある。ＭＰＳを共に構成する安全ブロックＩ及びＩＩは、ＣＣＦを１つのブロックに限定するために選択され得る。慣例的に、原子力発電所は、ＣＣＦによってＭＰＳが使用不能になった場合に機能を始動する多様な方法を提供するため、多様化作動システム（ＤＡＳ）又はスクラムなしの予想遷移（ＡＴＷＳ）に依存してきた。しかし、図示されたＭＰＳ設計において、単一のＣＣＦであっても安全機能を始動するのに十分な多様性がシステム内に存在し得る。ここで、ＭＰＳは、安全ブロックＩ及びＩＩ（例えば、１００６ａ／ｂ）に分割される。想定されるソフトウェア又はハードウェアＣＣＦは、１つの安全ブロックに限定されることになる。各ブロックは、異なるプログラマブル技術（設計及び機器多様性）に基づいて異なるプログラマブルデジタルハードウェアを利用する異なる設計チーム（人間多様性）を使用し、異なるプログラマブル技術は、異なる設計ツール（ソフトウェア多様性）の使用を必要とし得る。各ブロック内で、別個のＳＦＭ上に実装される、異なる物理効果の被測定変数に基づく少なくとも２つの安全機能が存在し得る。全ての論理は、有限状態機械に実装されてもよく、また、全ての安全データは、決定論的方法で通信されてもよい。これらの属性に起因して、ＣＣＦに関連する型３故障でも、ＭＰＳが必要な保護動作を始動することを妨げない可能性がある。

【０１９０】

別の分析指針は事故についての多様性である。ＡＯＯと同様に、ＭＰＳ内のＣＣＦエラーに関連する想定事故は、ＭＰＳがその安全機能を実行することを妨げない可能性がある

。

【０１９１】

別の分析指針は、手動オペレータ動作である。ＭＰＳによって実行される保護動作の手動区分レベル作動は、オペレータに提供されてもよい。手動コンポーネントレベル制御は、１Ｅ　Ｍ／Ｉによって許可される場合、非１Ｅ　Ｍ／Ｉを使用してオペレータに提供される。

【０１９２】

主題の特定の実装形態が述べられた。他の実装形態、代替形態、及び述べる実装形態の変更は、当業者にとって明らかであるように、以下の特許請求の範囲内にある。例えば、請求項に記載された動作は、異なる順序で実行され、またそれでも望ましい結果を達成し得る。したがって、例示的な実装形態の先の説明は、本開示を規定又は制限しない。他の変更形態、置換形態、及び代替形態もまた、本開示の精神及び範囲から逸脱することなく可能である。

【図面】

【図１】

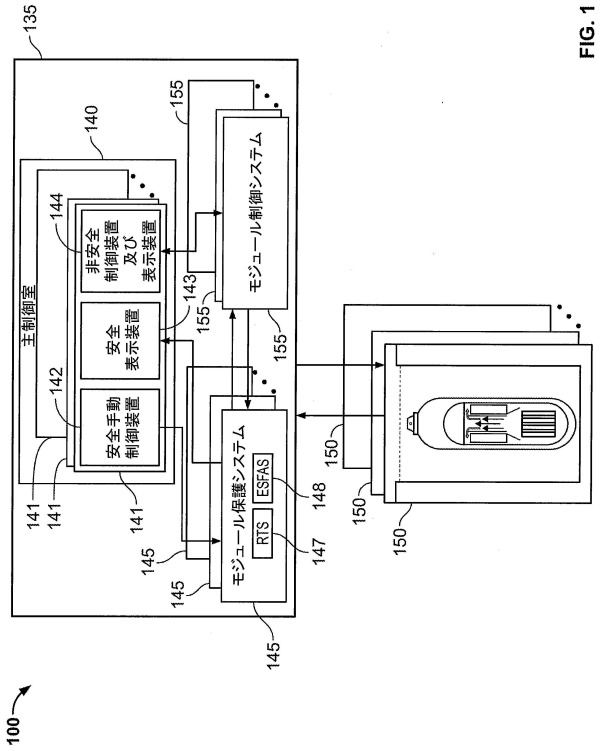


FIG. 1

【図２Ａ】

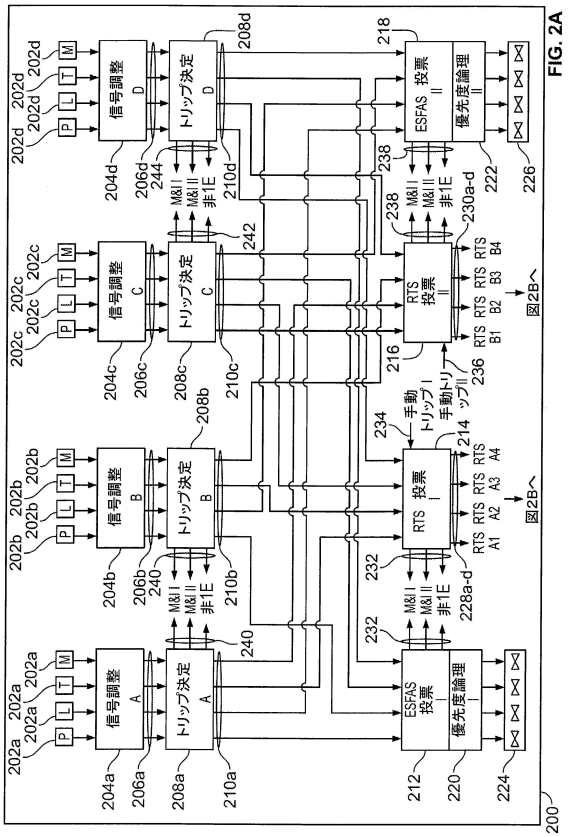


FIG. 2A

【図２Ｂ】

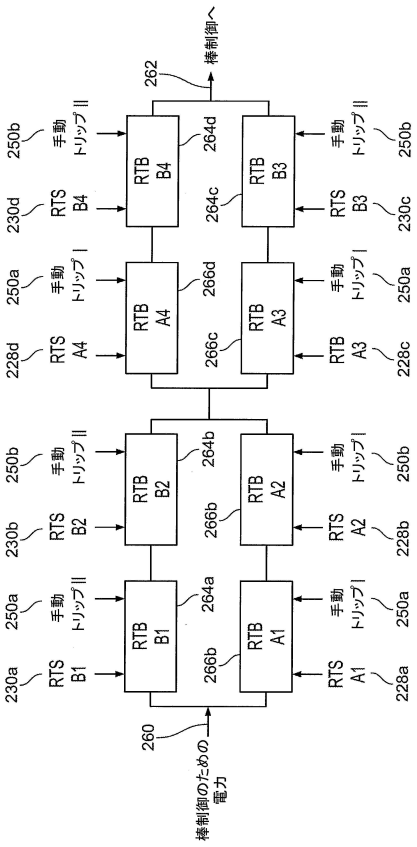


FIG. 2B

【図３Ａ】

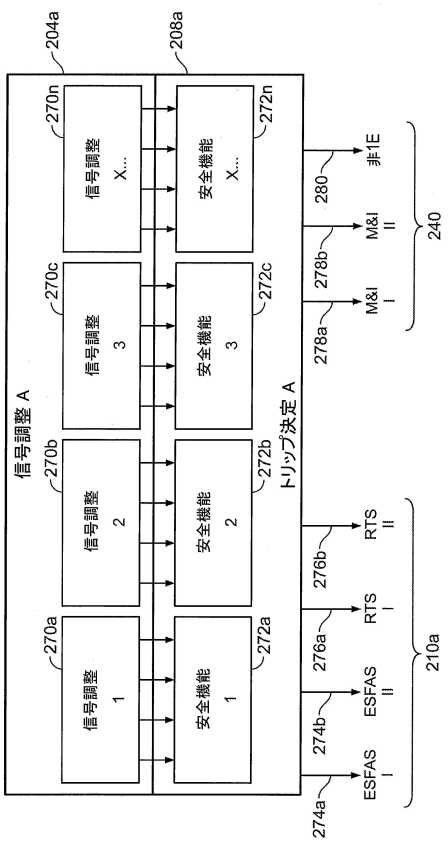


FIG. 3A

【図３Ｂ】

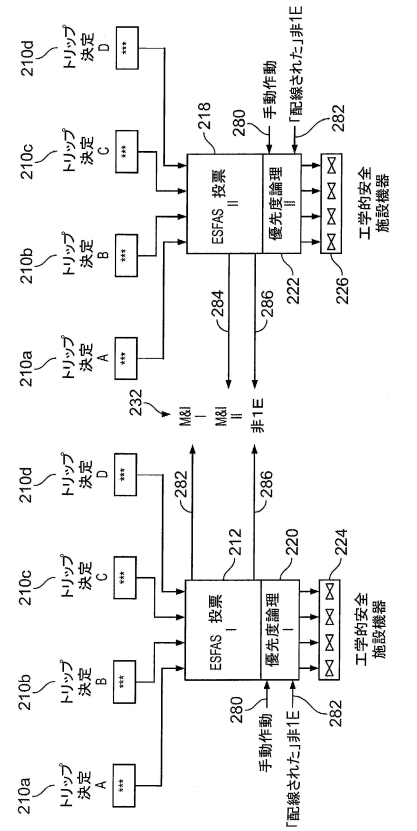


FIG. 3B

【図４Ａ－４Ｂ】

400

過渡事象	安全機能	プロセスパラメータ	分離グループ A	B	C	D	トリップ／トリップなし決定
給水喪失	A1	高温					トリップ
	A2	高圧					トリップ

FIG. 4A

450

過渡事象	安全機能	プロセスパラメータ	分離グループ A	B	C	D	トリップ／トリップなし決定
給水喪失	A1	高温	CCF		CCF		トリップ
	A2	高圧					トリップ

FIG. 4B

【図５】

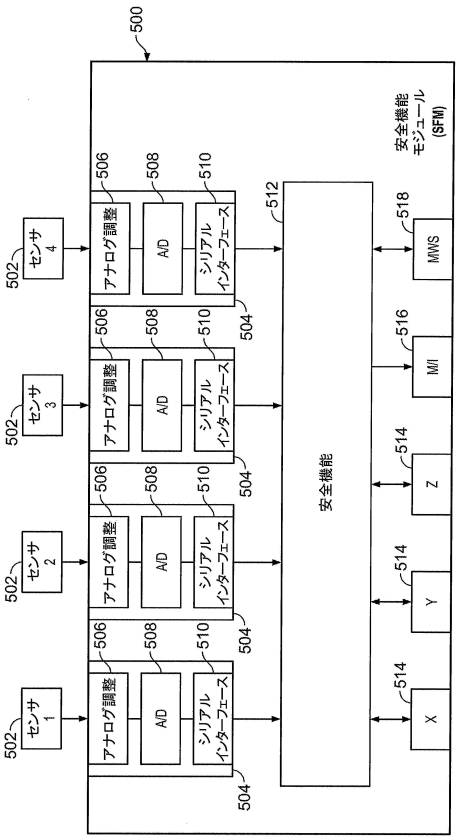


FIG. 5

【図６】

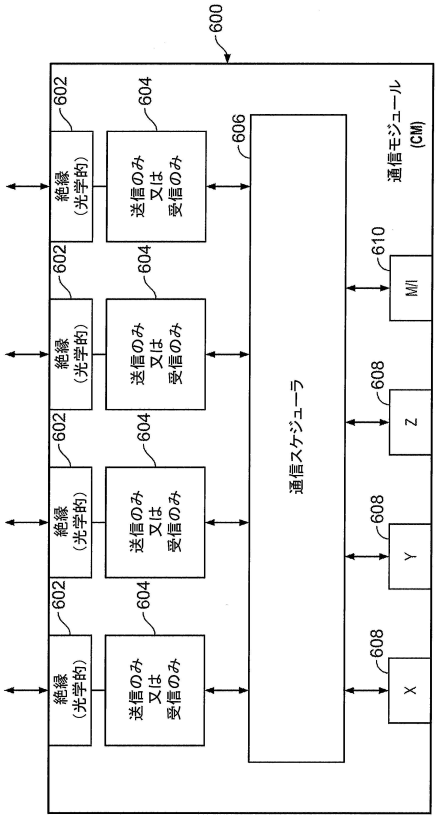


FIG. 6

【図７】

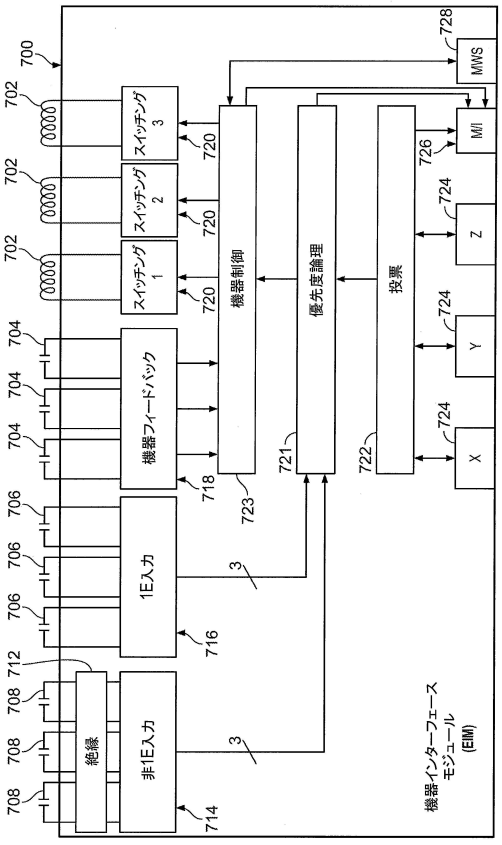


FIG. 7

【図８】

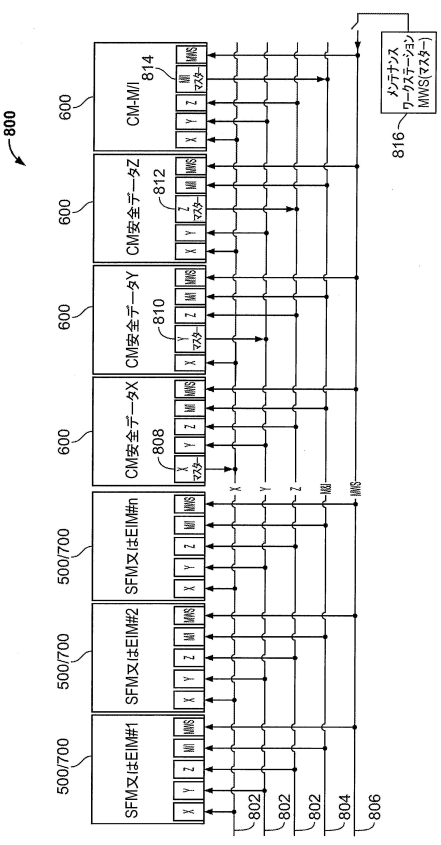


FIG. 8

【図９Ａ】

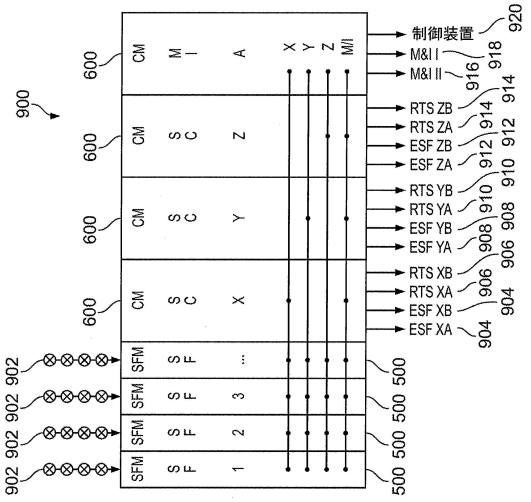


FIG. 9A

【図９Ｂ】

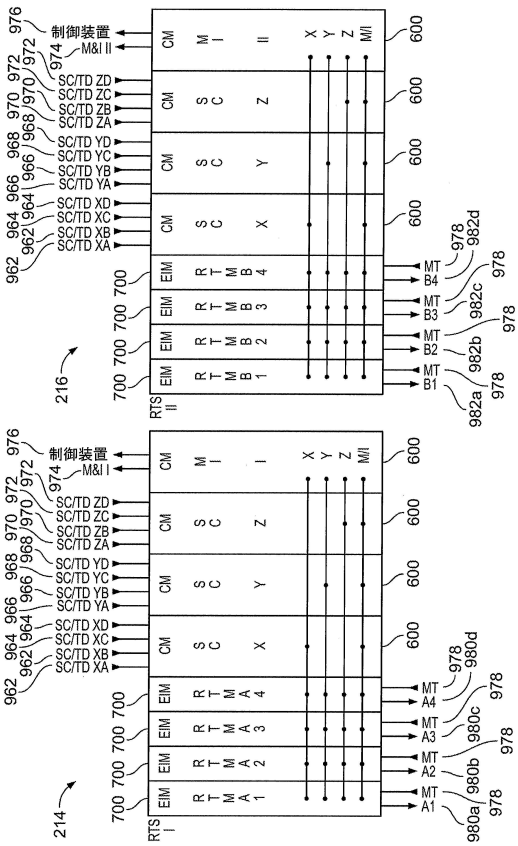


FIG. 9B

【図９Ｃ】

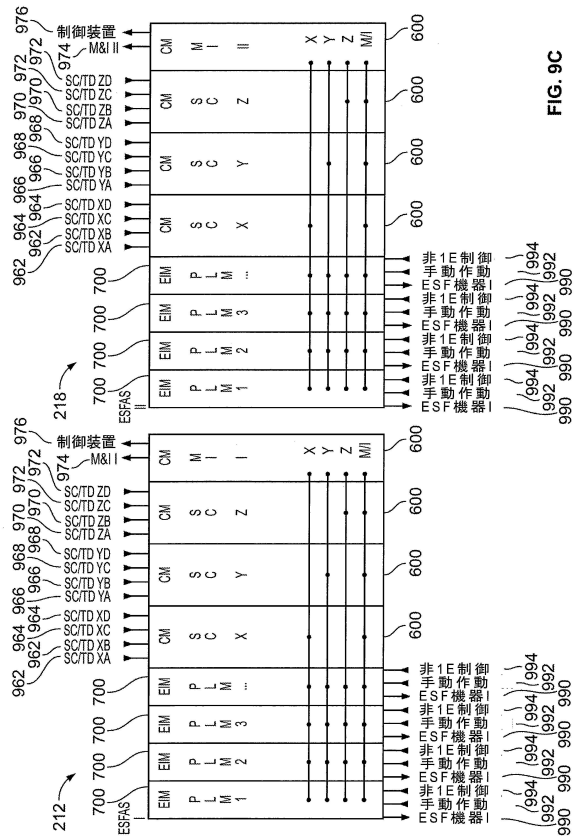


FIG. 9C

【図１０】

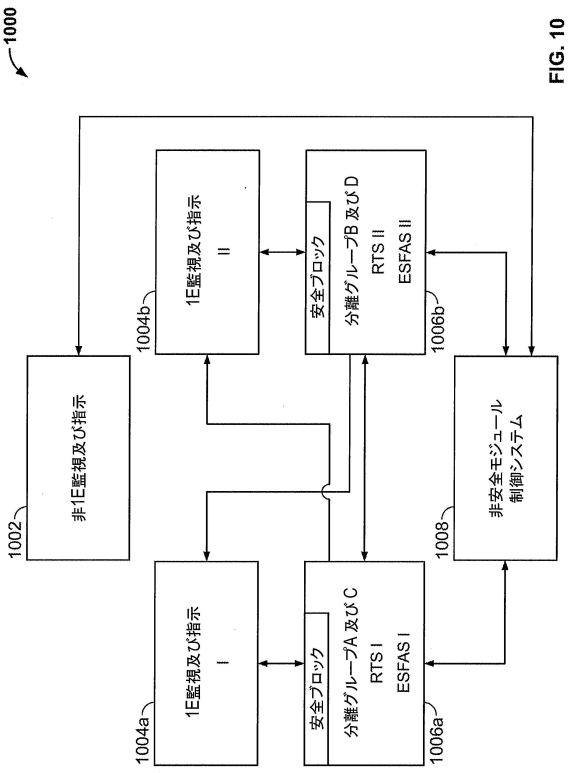


FIG. 10

【図１１】

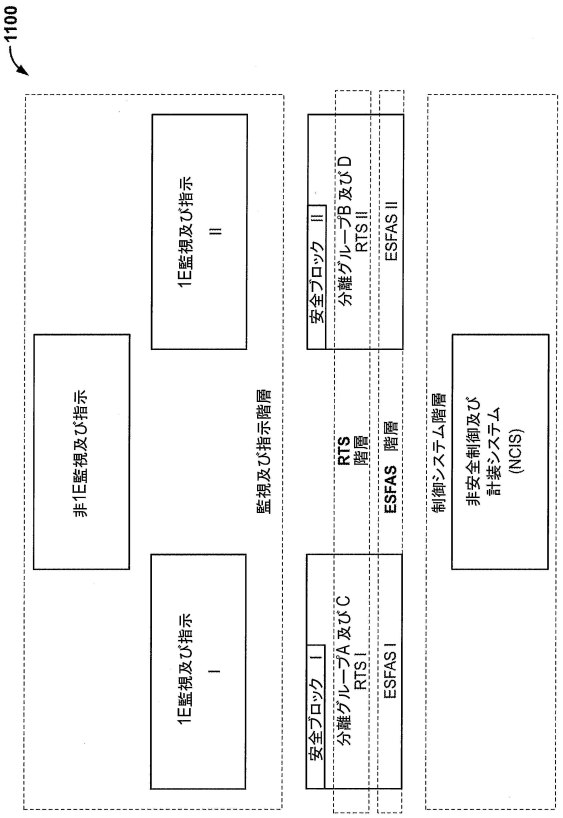

1100
非1E監視及び指示
1E監視及び指示 I
1E監視及び指示 II
監視及び指示階層
安全ブロック I
分離グループA及びC
RTS I
ESFAS I
安全ブロック II
分離グループB及びD
RTS II
ESFAS II
RTS 階層
ESFAS 階層
制御システム階層
非安全制御及び計装システム (NCIS)

FIG. 11

【手続補正書】
【提出日】令和5年1月19日(2023.1.19)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
原子炉保護システムであって、
安全システムからの第１セットの入力に少なくとも部分的に基づいて第１安全施設決定を導くハードウェア構成を有する第１論理回路であって、前記第１安全施設決定は、原子炉又はその一部分の推定状態を検出することに対応する、第１論理回路と、
前記第１論理回路に並列に通信可能に結合される第２論理回路であって、前記第２論理回路は、前記安全システムからの第２セットの入力に少なくとも部分的に基づいて第２安全施設決定を導くハードウェア構成を有し、前記第２安全施設決定は、異なる入力及び異なる回路を使用した前記推定状態の冗長な検出に対応する、第２論理回路と、
前記第１論理回路及び前記第２論理回路に通信可能に結合されて前記第１安全施設決定及び前記第２安全施設決定に基づいて前記推定状態に対処する原子炉安全アクチュエータとを含む、原子炉保護システム。
【請求項２】
前記第１論理回路及び前記第２論理回路は、これら論理回路の中の複数の回路コンポーネント間のハードウェア設定及び／又は接続が、前記第１安全施設決定及び前記第２安全施設決定それぞれを導くように事前に構成される、請求項１の原子炉保護システム。
【請求項３】
前記第１論理回路は、前記第１安全施設決定を導くハードウェア構成を有する第１フィールドプログラマブルゲートアレイ（ＦＰＧＡ）であり、
前記第２論理回路は、前記第２安全施設決定を導くようにハードウェアが構成される第２ＦＰＧＡを含む、請求項１の原子炉保護システム。
【請求項４】
前記第１ＦＰＧＡ及び前記第２ＦＰＧＡは、前記推定状態を決定するための異なる独立した処理構成を有する、請求項３の原子炉保護システム。
【請求項５】
前記第１ＦＰＧＡと前記第２ＦＰＧＡとは、ハードウェアの型、構成及び／又はアーキテクチャが異なる、請求項３の原子炉保護システム。
【請求項６】
前記第１ＦＰＧＡ及び前記第２ＦＰＧＡのハードウェアの構成が、異なるソフトウェア及び／又は異なるプラットフォームを使用して確立される、請求項３の原子炉保護システム。
【請求項７】
前記第１論理回路及び前記第２論理回路から前記第１安全施設決定及び前記第２安全施設決定を受け取るべく結合される投票回路をさらに含み、
前記投票回路は、前記第１安全施設決定及び前記第２安全施設決定を投票入力として解釈することに基づいて安全動作を決定するべく構成され、
前記安全動作は前記推定状態への応答を表し、
前記安全動作により前記原子炉安全アクチュエータが、前記推定状態に対処するべく動作する、請求項１の原子炉保護システム。
【請求項８】
前記第１論理回路は、
前記推定状態に関連付けられる論理決定に対応する第１決定出力を生成するべく構成され

る第１回路と、
前記推定状態に関連付けられる第１冗長論理決定に対応する第２決定出力を生成するべく構成される第２回路と、
前記推定状態に関連付けられる第２冗長論理決定に対応する第３決定出力を生成するべく構成される第３回路と
を含み、
前記第１回路、前記第２回路及び前記第３回路は、互いから電気的に分離されかつ独立して動作し、
前記投票回路は、前記第１決定出力、前記第２決定出力及び前記第３決定出力により示される値の多数に対応する前記安全動作を決定するべく構成され、
前記原子炉保護システムは、
前記第１回路を前記投票回路に結合する第１データバス経路と、
前記第２回路を前記投票回路に結合する第２データバス経路と、
前記第３回路を前記投票回路に結合する第３データバス経路と
をさらに含み、
前記第１データバス経路、前記第２データバス経路及び前記第３データバス経路は互いから分離かつ独立である、請求項７の原子炉保護システム。
【請求項９】
前記第１データバス経路を経由してデータ通信を制御することにより前記第１データバス経路のためのマスターとして機能するべく構成される第１通信モジュールと、
前記第２データバス経路を経由してデータ通信を制御することにより前記第２データバス経路のためのマスターとして機能するべく構成される第２通信モジュールと、
前記第３データバス経路を経由してデータ通信を制御することにより前記第３データバス経路のためのマスターとして機能するべく構成される第３通信モジュールと
をさらに含み、
前記第１データバス経路、前記第２データバス経路及び前記第３データバス経路は互いから分離かつ独立である、請求項８の原子炉保護システム。
【請求項１０】
前記第１論理回路及び前記第２論理回路に並列に通信可能に結合される第３論理回路をさらに含み、
前記第３論理回路は、安全システムからの第３セットの入力に少なくとも部分的に基づいて第３安全施設決定を導くハードウェア構成を有し、
前記第３安全施設決定は、異なる入力及び異なる回路を使用した前記推定状態のさらに冗長な決定に対応し、
前記投票回路は、前記第３論理回路に通信可能に結合されて第１階層投票結果及び第２階層投票結果に基づいて前記安全動作を決定するべく構成され、
前記第１階層投票結果は前記第１安全施設決定に対応し、前記第１決定出力、前記第２決定出力及び前記第３決定出力により示される値の前記多数として生成され、
前記第２階層投票結果は、前記第１安全施設決定、前記第２安全施設決定及び前記第３安全施設決定により示される一致値の最小数に対応する、請求項８の原子炉保護システム。
【請求項１１】
原子炉保護システムを動作させる方法であって、
原子炉又はその一部分を別個にモニタリングすることから第１セットの入力及び第２セットの入力を受信することと、
第１論理回路を使用して、前記第１セットの入力に少なくとも部分的に基づいて第１安全施設決定を導くことであって、前記第１安全施設決定は、前記原子炉又はその一部分の推定状態に対応することと、
第２論理回路を使用して、前記第２セットの入力に少なくとも部分的に基づいて第２安全施設決定を導くことであって、前記第２安全施設決定は、異なる入力及び異なる回路を使用した前記推定状態の冗長な検出に対応することと、

前記第１安全施設決定及び前記第２安全施設決定に基づいて、前記第１論理回路及び前記第２論理回路に通信可能に結合されるＥＳＦＡＳコンポーネントアクチュエータ又は原子炉トリップ遮断器の一方の作動状態を制御することであって、前記作動状態は前記推定状態に対処するべく制御されることと
を含む、方法。
【請求項１２】
前記第１安全施設決定を導くことは、前記第１論理回路のハードウェア構成に従って前記第１セットの入力を処理することを含み、
前記第２安全施設決定を導くことは、前記第２論理回路のハードウェア構成に従って前記第２セットの入力を処理することを含む、請求項１１の方法。
【請求項１３】
前記第１論理回路のハードウェア構成と前記第２論理回路のハードウェア構成との間の事前に構成された接続は異なる、請求項１２の方法。
【請求項１４】
前記第１論理回路と前記第２論理回路とは、回路コンポーネントが異なり、内部接続が異なり、ハードウェアの型が異なり、及び／又はアーキテクチャが異なる、請求項１３の方法。
【請求項１５】
前記第１論理回路は第１フィールドプログラマブルゲートアレイ（ＦＰＧＡ）であり、
前記第２論理回路は第２ＦＰＧＡである、請求項１１の方法。
【請求項１６】
前記第１ＦＰＧＡ及び前記第２ＦＰＧＡは、ハードウェアの構成を確立するべく使用される異なるコンポーネントに対応する、請求項１５の方法。
【請求項１７】
第１セットの冗長回路を使用して、前記第１セットの入力に部分的に基づいて一セットの第１冗長安全施設決定を導くことであって、前記第１セットの冗長回路における各回路は、前記第１セットの冗長回路における他の回路から及び前記第１論理回路から分離かつ独立であることをさらに含み、
前記作動状態は、前記第１安全施設決定及び前記一セットの第１冗長安全施設決定により示される値の多数に従って制御される、請求項１１の方法。
【請求項１８】
単一箇所通信故障を防止するべく専用バスを経由して前記第１安全施設決定及び各冗長決定の通信を独立して制御することをさらに含む、請求項１７の方法。
【請求項１９】
前記原子炉又はその一部を別個にモニタリングすることから第３セットの入力を受信することと、
第３論理回路を使用して、前記第３セットの入力に少なくとも部分的に基づいて第３安全施設決定を導くことと
を含み、
前記第３安全施設決定は、異なる入力及び異なる回路を使用した前記推定状態のさらに冗長な検出に対応し、
前記作動状態は、前記第１安全施設決定、前記第２安全施設決定及び前記第３安全施設決定により示される一致する値の最小数に従って制御される、請求項１１の方法。
【請求項２０】
それぞれが前記推定状態に対応する前記第１安全施設決定、前記第２安全施設決定及び前記第３安全施設決定に基づいて前記作動状態を制御することは、単一箇所ハードウェア関連故障を防止し又は単一箇所ハードウェア関連故障から回復することを含む、請求項１９の方法。
【外国語明細書】

フロントページの続き

弁理士　大渕 一志
(72)発明者　クラークソン グレゴリー ウェイン
アメリカ合衆国 カンザス州 ６６８３９ ニュー ストローン オーセージ ストリート １１７
(72)発明者　アヤラ ルフィーノ
アメリカ合衆国 カンザス州 ６６８３９ ニュー ストローン オーセージ ストリート １１７
(72)発明者　ポトフ ジェイソン
アメリカ合衆国 オレゴン州 ９７３３０ コーバリス ノースイースト サークル ブルバード １１００ スイート ２００