(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5285146号
(P5285146)

(45)発行日　平成25年9月11日(2013.9.11)　(24)登録日　平成25年6月7日(2013.6.7)

(51)Int.Cl.　F I
B60R 21/264 (2006.01)　B60R 21/264
B60R 21/01 (2006.01)　B60R 21/01　100

請求項の数 15　(全 14 頁)

(21)出願番号　特願2011-510590 (P2011-510590)
(86)(22)出願日　平成21年5月15日(2009.5.15)
(65)公表番号　特表2011-520702 (P2011-520702A)
(43)公表日　平成23年7月21日(2011.7.21)
(86)国際出願番号　PCT/US2009/044069
(87)国際公開番号　WO2009/142997
(87)国際公開日　平成21年11月26日(2009.11.26)
審査請求日　平成23年1月18日(2011.1.18)
(31)優先権主張番号　12/154,122
(32)優先日　平成20年5月20日(2008.5.20)
(33)優先権主張国　米国(US)

(73)特許権者　598122843
オートリブ　エー・エス・ピー・インク
アメリカ合衆国　ユタ州８４４０５，オグデン市，エアポートロード３３５０
(74)復代理人　110000349
特許業務法人　アクア特許事務所
(74)代理人　503175047
オートリブ株式会社
(72)発明者　エイスワース、　デビッド
アメリカ合衆国　ミシガン州　４８３９３、　ウィクソム、　２０３５　メディナドライブ

最終頁に続く

(54)【発明の名称】自動車の火工的安全装置を廃棄するフェイルセーフ装置および方法

(57)【特許請求の範囲】
【請求項１】
火工的安全装置廃棄方法において、
基本制御装置と、セーフィングモードおよびスクラップモードを含む補助制御装置を含む電子制御装置とを準備し、
前記補助制御装置が前記基本制御装置から第１の所定信号を受信した時に前記スクラップモードをオンにし、
前記補助制御装置が前記スクラップモードにて作動している時に前記基本制御装置からの第２の所定信号を前記補助制御装置が受信した場合のみ、前記補助制御装置を発火させ、
前記補助制御装置の発火中に少なくとも１つの前記火工的装置に展開信号を送信することにより、少なくとも１つの火工的装置を展開させることを特徴とする火工的安全装置廃棄方法。
【請求項２】
請求項１に記載の方法において、前記展開信号は、前記基本制御装置が外部ソースから信号を受信した後に、前記基本制御装置から送信することを特徴とする方法。
【請求項３】
請求項２に記載の方法において、前記外部ソースがＣＡＮベースのテスタであることを特徴とする方法。
【請求項４】

請求項３に記載の方法において、前記基本制御装置は、外部ソースから第１の信号を受信した後に前記第１の所定信号を送信し、前記外部ソースから第２の信号を受信した後に前記第２の所定信号を送信することを特徴とする方法。

【請求項５】

請求項４に記載の方法において、前記外部ソースがＣＡＮベースのテスタであり、前記ＣＡＮベースのテスタは前記補助制御装置と電気通信を行わないことを特徴とする方法。

【請求項６】

請求項１に記載の方法において、前記第２の所定信号と前記展開信号とを同時に送信すること特徴とする方法。

【請求項７】

請求項１に記載の方法において、さらに、

基本制御装置のメモリ内に、複数の所定信号に相当する符号化データを保存し、

外部ソースから前記基本制御装置が受信した複数の信号に基づいた復号キーを決定し、

前記第１および第２の所定信号に相当する、前記符号化データの少なくとも一部分を前記復号キーを用いて復号することを特徴とする方法。

【請求項８】

請求項７に記載の方法において、前記復号キーは、前記外部ソースから前記基本制御装置が受信した前記複数の信号の各々の１６進値に基づいて決定することを特徴とする方法。

【請求項９】

請求項７に記載の方法において、前記符号化データは、実行可能な形式に復号することを特徴とする方法。

【請求項１０】

請求項７に記載の方法において、さらに、

廃棄セッションが終了した時に前記補助制御装置を前記セーフィングモードにリセットし、

前記復号キーおよび前記復号データを破棄することを特徴とする方法。

【請求項１１】

請求項１０に記載の方法において、前記電子制御装置をリセットするか、前記電子制御装置へのパワーを喪失させるか、あるいは前記外部ソースとの通信を喪失させることによって、前記廃棄セッションを終了させることを特徴とする方法。

【請求項１２】

請求項１に記載の方法において、さらに、

前記補助制御装置の発火中に前記基本制御装置が前記展開信号を受信した時は、少なくとも１つの火工的装置の第１の火工的装置が展開した後に、前記補助制御装置を安全化し、

廃棄信号を前記基本制御装置が受信したときのみ、前記補助制御装置を再発火させ、

前記基本制御装置が前記外部ソースから前記廃棄信号を受信した時、第２の火工的装置を展開させることを特徴とする方法。

【請求項１３】

請求項１２に記載の方法において、前記基本制御装置にいずれかの非廃棄信号を送信することにより、前記補助制御装置を安全化することを特徴とする方法。

【請求項１４】

請求項１２に記載の方法において、前記補助制御装置を所定の時間発火させることを特徴とする方法。

【請求項１５】

火工的安全装置の廃棄システムにおいて、

補助制御装置および基本制御装置を含む電子制御装置であって、前記基本制御装置は前記補助制御装置と電気通信を行い、前記補助制御装置はセーフィングモードおよびスクラップモードで作動するよう構成される電子制御装置と、

前記補助制御装置および前記基本制御装置と電気通信を行う火工的安全装置と、
前記基本制御装置と電気通信を行い、前記補助制御装置と電気通信を行わない、外部信号装置とを含み、
前記補助制御装置が第１の所定信号を前記基本制御装置から受信した時、前記補助制御装置は、前記セーフィングモードから前記スクラップモードに切り換わるよう構成され、前記補助制御装置は、前記補助制御装置が前記基本制御装置から第２の所定信号を受信し前記補助制御装置が前記スクラップモードで作動している時に、前記火工的安全装置を発火させるよう構成されることを特徴とする、火工的安全装置の廃棄システム。
【発明の詳細な説明】
【背景】
【０００１】
本発明は、全体として、火工的安全装置の廃棄、とりわけフェイルセーフな自動車用火工的安全装置の廃棄に関する。
【０００２】
自動車は、通常、自動安全装置を含んでいて、さまざまな火工的安全装置（ＰＳＤ）および一連の衝突センサを搭載している。万一の自動車衝突の場合には、衝突センサから受信した信号に反応してＰＳＤが作動すなわち展開し、自動車の乗員が被る負傷を和らげる。ＰＳＤの例としては、エアバッグ、シートベルト・プリテンショナ、展開可能ロールバー、展開可能ニーボルスタ、展開可能アンチサブマリン装置、「ポップアップ」式歩行者安全フードなどがある。
【０００３】
自動車の耐用年数の終了時、展開しなかった多数の「生きている」ＰＳＤが自動車に残る。ＰＳＤの火工的性質のため、多くの国の政府規則で、安全上の理由から、ＰＳＤの除去、保管および再利用を禁じている。近年、多くの政府が、展開しなかったＰＳＤを残している自動車の廃棄を禁じる規則をも施行し、今や、自動車廃棄の前に、展開しなかったすべてのＰＳＤを展開させるよう求めている。このような規則の１つは、ＩＳＯ　２６０２１規約案に盛り込まれていて、自動車拘束システムコントローラが、外部装置からＰＳＤ廃棄命令を受信し、それに基づいて作動することを求めている。
【０００４】
自動車拘束システムの主要な目的は衝突時に自動車の乗員の負傷を和らげることであるから、明白な自動車の衝突状態、すなわち乗員の負傷を引き起こすほど重大な衝突状態が認識された時のみ、ＰＳＤを作動させることが望ましい。
【０００５】
ＰＳＤの偶発のもしくは不要な展開を防ぐために、自動車拘束システムコントローラは一般に「フェイルセーフ」に設計され、システムの構成要素のうちただの１つも、ＰＳＤへ流れる展開電流を生じさせる工程で失敗しないように設計される。全体として、このフェイルセーフ構造は、多数の独立した衝突センサ、ロジック回路評価、および展開コントロールハードウェアをアレンジすることにより実現され、個々の構成要素それぞれが所定の展開状態に達したときしか、展開電流が流れることを許容しない。しかし、自動車拘束システムコントローラのこのフェイルセーフ構造によって、自動車の廃棄に先立って手動で安全にＰＳＤを廃棄することが困難になっている。なぜなら、一般的に、衝突状態を示すセンサ入力がなければ、所定の展開状態にならないからである。
【０００６】
このように、標準的な拘束システム構造は、ＰＳＤ廃棄用の展開が単一の通信ポートを介して制御されることを求めるＩＳＯ　２６０２１規約案などの規則とは矛盾している。単一の通信ポートを介した展開を実現するには、関連する制御ロジックが、多くの自動車拘束システムコントローラ内蔵のインターロックおよびリダンダンシを実質的に無視する必要がある。しかしこれにより、仮に個々の構成要素の故障モードが適切に管理されなかった場合には、システムの偶発的な展開の危険性が潜在的に増すことになってしまう。
【０００７】

したがって、ＩＳＯ　２６０２１規約案などの新しい政府規則に準拠する、火工的安全装置の廃棄のためのフェイルセーフ方法および装置に対するニーズが現存する。

【発明の概要】

【０００８】

本発明の一面において、火工的安全装置の廃棄に関する方法は、基本制御装置および補助制御装置を有する電子制御装置を設けることを含んでよい。補助制御装置はセーフィングモードおよびスクラップモードを含み、初期状態ではセーフィングモードで作動する。補助制御装置は、基本制御装置から第１の所定信号を受信すると、セーフィングモードからスクラップモードに切り換わる。補助制御装置は、補助制御がスクラップモードで作動している間に基本制御装置から第２の所定信号を受信したときのみ、発火する。補助制御装置の発火中に単一のＰＳＤへ展開信号を送信することにより、その単一のＰＳＤを展開させる。

【０００９】

他の側面において、展開信号は、外部ソースより受信した信号に基づき、基本制御装置からＰＳＤへ送信する。基本制御装置は、外部信号ソースから第１の信号を受信した後に、第１の所定信号を補助制御装置に送信する。基本制御装置は、外部信号ソースから第２の信号を受信した後に、第２の所定信号を補助制御装置に送信する。外部信号ソースはＣＡＮベースのテスタとしてよく、補助制御装置とは通信不能である。

【００１０】

さらに本発明の他の側面において、火工的安全装置の廃棄方法は、基本制御装置のメモリに符号化データを保存することを含んでよい。符号化データは複数の所定信号に相当する。復号キーは、基本制御装置が外部信号ソースから受信する複数の信号に基づいて決定される。第１および第２の所定信号に相当する、符号化データの少なくとも一部分は、この復号キーを使って復号される。

【００１１】

本発明の他の側面において、補助制御装置は、廃棄セッションが終了するとセーフィングモードにリセットされ、復号キーおよび復号データが破棄可能となる。

【００１２】

本発明による火工的安全装置の他の処理方法は、基本制御装置および補助制御装置を含む電子制御装置を設けることを含み、補助制御装置はセーフィングモードおよびスクラップモードで作動可能である。補助制御装置がスクラップモードで作動する時、補助制御装置から基本制御装置へ廃棄シードが送信される。廃棄シードに基づいて廃棄キーが計算され、補助制御装置は、基本制御装置が廃棄キーを補助制御装置に送信した時に発火する。火工的装置の発火中に展開信号を単一の火工的装置に送信することにより、その単一の火工的装置が展開する。廃棄キーは、ユニークな定期的メッセージとしてよい。

【００１３】

１つの実施形態では、補助制御装置は展開後に安全化させてよい。また、仮に他の廃棄信号を基本制御装置より受信した場合には、再発火させてよい。第２の火工的装置は、補助制御装置が廃棄信号を受信したときに展開させてよく、補助制御装置の発火中、基本制御装置は火工的装置に展開信号を送信する。

【００１４】

火工的安全装置の廃棄に関するシステムは、補助制御装置および基本制御装置を有する電子制御装置を含んでよい。基本制御装置は補助制御装置と電気通信を行い、補助制御装置はセーフィングモードおよびスクラップモードで作動するように構成される。また本システムは、補助制御装置および基本制御装置と電気通信を行う火工的安全装置と、基本制御装置と電気通信を行う外部信号装置とを含む。外部信号装置は、補助制御装置と電気通信を行わない。１つの実施形態では、外部信号装置はＣＡＮベースのテスタとしてよい。

【００１５】

補助制御装置は、補助制御装置が基本制御装置から第１の所定信号を受信した時に、セーフィングモードからスクラップモードに切り換わるよう構成される。また補助制御装置

は、補助制御装置がスクラップモードで作動している時に基本制御装置から第２の所定信号を受信すると、火工的安全装置を発火させるよう構成される。

【００１６】

さらに他の一面では、発火後、決まった期間だけ補助制御装置の発火状態を継続させてよい。

【００１７】

概要の紹介として以上の各段落を記載したが、後述する特許請求の範囲を制限する意図はない。現状の好ましい実施形態は、他の利点とともに、以下に続く詳細な説明および添付の図面を参照して、最もよく理解可能である。

【図面の簡単な説明】

【００１８】

本発明は、図面と関連した以下の説明を読むことにより、より完全に理解可能である。

【図１】図１（ａ）は本発明の実施形態による電子制御装置に関するシステム図である。図１（ｂ）は図１（ａ）の電子制御装置に関するタイミング図である。

【図２】火工的安全装置の廃棄に関するフェイルセーフ方法のフローチャートである。

【図３】補助制御装置が図２のセーフィングモードで作動している時に火工的安全装置を展開させる工程に関する詳細なフローチャートである。

【図４】補助制御装置が図２のスクラップモードで作動している時に火工的安全装置を展開させる工程に関する詳細なフローチャートである。

【図５】補助制御装置が図２のスクラップモードで作動している時に第２の火工的安全装置を展開させる工程に関するフローチャートである。

【図６】補助制御装置の作動形態がスクラップモードで作動している時の第１および第２の火工的安全装置の展開に関する典型的なタイミング図である。

【図７】本発明による、補助制御装置の作動形態に関する論理図である。

【発明の詳細な説明】

【００１９】

「火工的安全装置」もしくは「ＰＳＤ」という用語は、火工品を含むあらゆる自動車安全拘束のことを指し、例えば、エアバッグ、シートベルト・プリテンショナ、展開可能ロールバー、展開可能ニーボルスタ、展開可能アンチサブマリン装置、「ポップアップ」式歩行者安全フードなどがあるが、これらに限られない。用語「展開」、「展開した」、「廃棄」およびこれらの派生語は、火工的安全装置の発火後の状態、つまり発生した火工ガスが実質的にすべて酸化した状態を指す。

【００２０】

最近の火工的安全装置は電子制御装置（ＥＣＵ）を含み、これは一般に２つのハードウェア制御装置、つまり、主要なマイクロコントローラ（ＭＣＵ）および独立した補助制御装置を利用する。補助制御装置はセーフィングロジックとも呼ばれ、衝突状態を認識し、各ＰＳＤを展開させる。一般的に、ＭＣＵはマイクロコントローラ衝突アリゴリズムを利用して衝突信号を分析し、衝突の位置および程度を決定する。衝突アルゴリズムが、衝突が十分重大であると判断した場合、ＭＣＵは、検知された衝突位置に相当するＰＳＤに展開信号を送信する。補助制御装置は、同時に独立して同衝突信号を分析し、衝突信号を有効にし、セーフィング（発火）をオンにする。ＰＳＤの展開を実現するためには、展開信号およびセーフィングが同時に発生しなければならない。

【００２１】

ＩＳＯ　２６０２１規約案などの政府規則および工業規格では、自動車が道路での使用に適さなくなった時および自動車がスクラップされる時に、展開されなかった、もしくは「生きている」ＰＳＤを廃棄するメカニズムをＥＣＵが有することを要求する。これらの規則の下では、スクラップ時に、テスタがコントローラ・エリア・ネットワーク（ＣＡＮ）を介してＥＣＵにメッセージ（信号）を送信し、ＰＳＤの廃棄を要求する。しかし、ＣＡＮメッセージはＭＣＵでしか受信されないため、補助制御装置は、テスタメッセージを同時に有効にするための外部入力を持たない。したがって本発明は、外部信号ソースから

送信されＭＣＵのみが受信する信号を独立して有効にし、これにより、「スクラップ時」に独立したセーフィングおよびＰＳＤの展開を実現することを目的とする。

【００２２】

各要素を示す参照番号については、図を参照されたい。図１（ａ）は、本発明の実施形態による電子制御装置（ＥＣＵ）１００を示している。ＥＣＵ１００は、補助制御装置１１０、基本マイクロコントローラ（ＭＣＵ）１２０およびＡＮＤゲート１８０を含む。補助制御装置１１０は、メモリに保存された２つの作動モード、つまり、セーフィングモード１１２およびスクラップモード１１４を含む。ＭＣＵ１２０は、衝突アルゴリズム１２２およびメモリに保存されたスクラップ管理データ１２４を含む。スクラップ管理データ１２４は、好ましくは、ＭＣＵ１２０のメモリ内に、実行不能形式にて符号化され保存される。補助制御装置１１０およびＭＣＵ１２０は、互いに双方向電気通信を行い、補助制御装置１１０およびＭＣＵは両方とも、自動車のＰＳＤと電気通信を行う（図示せず）。ＡＮＤゲート１８０もまた、ＭＣＵ１２０および補助制御装置１１０と同様、自動車のＰＳＤと電気通信を行う。

【００２３】

補助制御装置１１０は、セーフィングモード１１２およびスクラップモード１１４の２つのうち１つのモードで、自動車のＰＳＤを発火もしくは安全化させるよう構成される。補助制御装置１１０はまた、ＭＣＵ１２０が補助制御装置１１０に廃棄シード１３０の要求を送信した時に、廃棄シード１３０をＭＣＵ１２０に送信するよう構成される。廃棄シード１３０は、好ましくは、シリアル・ペリフェラル・インタフェース（ＳＰＩ）を介して、２ｋＨｚに等しいかそれ以上のスピードで送信される。補助制御装置１１０は、ＣＡＮを介して送信された信号、もしくは、テスタなどの、ＥＣＵ１００の外部ソースから他の通信ラインを受信できないことが好ましい。

【００２４】

ＭＣＵ１２０は、複数の自動車衝突センサ（図示せず）からの信号、ならびにテスタ（図示せず）などの外部信号ソースからの信号、廃棄シード１３０を含む補助制御装置１１０からの信号を受信するよう構成される。ＭＣＵ１２０はＣＡＮを介して外部信号を受信することが好ましい。しかし、現存するもしくは後に開発されるいかなる電気通信ラインを信号送信に利用してもよいと理解すべきであり、例えばこれらに限られないがイントラネット、ケーライン、もしくはワイヤレス・プロトコルを含む。ＭＣＵ１２０はまた、自動車のＰＳＤに信号を送信し、廃棄キー１４０などの信号を補助制御装置１１０に送信するよう構成される。信号は、シリアル・ペリフェラル・インタフェース（ＳＰＩ）を介して送信されることが好ましい。

【００２５】

作動に際して、廃棄シード／廃棄キーによる方法を用いて、補助制御装置１１０がスクラップモード１１４で作動中に補助制御装置１１０を発火させてよい。これについての詳細は、図２～図５を参照して下記に述べる。

【００２６】

図１（ｂ）は、補助制御装置１１０と、ＥＣＵ１００のＭＣＵ１２０とのタイミング動作を示している。時刻t_0では、偶発の展開を避けるために、安全化機能１５０はＨＩＧＨであり、発火機能はＬＯＷである。補助制御装置１１０は、時刻t_1で初めて発火機能１６０を作動させる。これは、セーフィングモード１１２で作動中に衝突センサ信号がＰＳＤ展開要求を満たしていると独立して確認すると同時に行われる。あるいは、スクラップモード１１４で作動中に廃棄キー信号を受信すると同時に行われる。補助制御装置１１０が時刻t_1で発火する時、安全化はＬＯＷで、発火はＨＩＧＨである。補助制御装置１１０の発火中、つまり時刻t_1～t_2の間、ＭＣＵ１２０は、時刻t_3～t_4間ではＨＩＧＨになる展開信号１７０を送信する。ＰＳＤは、展開信号がＨＩＧＨでありかつ補助制御装置１１０の発火機能１６０がＨＩＧＨである場合のみ、展開可能である。展開信号がＨＩＧＨであり、発火機能１６０がＬＯＷであり、安全化機能１５０がＨＩＧＨである場合、ＰＳＤは展開できない。図１（ｂ）に見られるように、発火すると、補助制御装置１

１０は所定の時間発火可能である。例えば、補助制御装置が発火したままでいる時間を定義した時刻t_1～t_2間のセーフィング・ウィンドウ（発火ウィンドウ）は、およそ０．５ミリ秒からおよそ２ミリ秒の間でよい。好ましくは、補助制御装置１１０を発火させている時間は、次の数式により計算される。

発火時間＝発火リード時間＋発火電流時間＋発火ラグ時間

【００２７】

ここで発火リード時間は、補助制御装置１１０が発火した後に展開信号がＰＳＤに送信されるように決定される。発火リード時間は、例えばおよそは、２ミリ秒からおよそ５ミリ秒の間でよいがこれに限られない。発火電流時間はハードウェアに依存し、パラメータを固定された火工装置に依存する。また、発火電流時間は、およそ０．５ミリ秒からおよそ２ミリ秒の間に設定してよい。発火ラグ時間（発火後の）は、補助制御装置１１０の発火継続を許容する追加の時間であり、この発火継続によって、ＰＳＤ展開に必要な時間が所定の発火電流時間では不足することになっても、確実にＰＳＤの展開が完了する。発火ラグ時間は、発火電流時間の複数倍としてよい。例えば、発火ラグ時間は発火電流時間の２倍としてよいが、これに限定されない。無論、セーフィング・ウィンドウは他の手段によって計算してもよく、もしくは、固定時間としてもよいことは理解されるべきである。例えば、発火ラグ時間は、およそ２ミリ秒からおよそ３ミリ秒の固定値であってもよい。

【００２８】

発火電流は、バッテリにより充電されるコンデンサによって提供してよい。コンデンサに蓄えられたチャージは、新しい発火電流がＰＳＤに送信される度に減少するため、コンデンサは、例えば、１６個のＰＳＤのうち１２番目のＰＳＤが発火した後、放電させてもよい。この場合、発火命令はＳＰＩ経由で送信されるが、実際の発火電流は、コンデンサが十分なボルテージにまで再充電された後に、ＰＳＤにのみ送信される。このように、補助制御装置１１０の発火中に発火信号をＰＳＤに確実に送信するために、また、ＰＳＤを確実に展開させるために、補助制御装置１１０の発火時間は、発火電流時間を超過することが望ましい。さらには、コンデンサは一般に経時劣化するので、発火ラグ時間を、コンデンサの劣化した性能を相殺するために作用させてもよい。

【００２９】

図２は、図１（ａ）の実施形態に従って、火工的安全装置の廃棄に関するフェイルセーフ方法を表すフローチャート例を示している。工程２１０において、補助制御装置１１０、ＭＣＵ１２０およびＡＮＤゲート１８０を含むＥＣＵ１００が、パワーオンされる。補助制御装置１１０は、２つのモード、つまり、セーフィングモード１１２およびスクラップモード１１４で作動するよう構成される。ＭＣＵ１２０は、メモリ、好ましくはＲＯＭを含んでよい。メモリは符号化データ１２４を保存していて、これは、補助制御装置１１０のスクラップモードをオンにしたり、ＰＳＤの火工的展開を命令したりするのに必要なものであり、好ましくは実行不能形式で保存される。工程２２０に見られるように、起動時、補助制御装置１１０はセーフィングモード１１２に設定され、衝突アルゴリズム１２２がオンになる。工程２３０において、ＭＣＵ１２０は、スクラップモード１１４に入るための外部信号をテスタ等から受信したか否かを判定する。

【００３０】

工程２４０に見られるように、外部信号が受信されなかったら、補助制御装置１１０はセーフィングモードを維持し、ＭＣＵ１２０はスクラップモード１１４に入るための外部信号を監視し続ける。しかし、スクラップモード１１４に入るための外部信号を受信したことをＭＣＵ１２０が判定すると、ＭＣＵ１２０は、スクラップモード１１４の入力に関するＩＳＯ　２６０２１規約案により定義された条件を満たすか否かを判定する。これは工程２５０に示される。仮に所定の条件を満たしていなかったら、補助制御装置はセーフィングモード１１２を維持し、ＭＣＵ１２０はスクラップモード１１４に入るための新しい外部信号を監視し続ける。

【００３１】

スクラップモード１１４に入るための所定の条件が満たされた場合、ＭＣＵ１２０は、

蓄積されたデータに基づく復号キー（図示せず）の組立を開始する。本データは、工程２６０に見られるように、ＣＡＮを介して外部信号ソースによって受信された信号を通じてＭＣＵ１２０が受信したものである。復号キーは、外部信号ソースによってＭＣＵ１２０に送信されたＣＡＮ信号（メッセージ）の１６進値のみから得られることが望ましい。また、外部信号ソースから外部ＣＡＮ信号を受信する前は、ＭＣＵ１２０のメモリ内には復号キーのいずれの部分も含まれていない、すなわち保存されていないことが望ましい。また、スクラップ状態を包括的に認識するのに必要なあらゆるＣＡＮメッセージが含まれるように、復号キーを選択することが望ましい。

【００３２】

工程２７０において、一旦復号キーの組立が完了すると、ＭＣＵ１２０は、ＭＣＵ１２０のＲＯＭに保存された符号化データ１２４を、実行可能な形式の指示に復号し、ＲＡＭに当該指示をロードする。復号された実行可能な指示には、セーフィング・ハードウェアにて展開制御を定期的に管理するアルゴリズム、火工的展開を命令するための指示、廃棄キー１４０を計算するための指示、および補助制御装置の作動モードを制御するための所定信号を含めてよい。ＭＣＵ１２０は、復号キーの適切さを確認できないことが望ましく、したがって、復号された実行可能な指示の適切さを確認できないことが望ましい。ＭＣＵ１２０は、単にＣＡＮ信号からの復号キーを組み立て、符号化されたデータ１２４を復号する。

【００３３】

指示がＲＡＭに一旦ロードされると、ＭＣＵ１２０は、符号化データ１２４から復号された所定信号を、復号キーを使って補助制御装置１１０に送信する。すると補助制御装置１１０はスクラップモード１１４をオンにする命令を出す。スクラップモード１１４に入ると、すべての衝突アルゴリズム１２２が中断され、補助制御装置１１０は、衝突センサからの信号の監視を停止する。所定信号は、補助制御装置１１０に、ＭＣＵ１２０から廃棄キー１４０を受信したときにのみ発火するよう命じる。このことは、図４に関連して後述する。

【００３４】

図３に注目すると、図３は図２のセーフィングモード実行２２０のフローチャートを示している。これは、非スクラップ状態における補助制御装置１１０の標準作動モードであり、ＥＣＵ１００がパワーオンされたときの初期モードと同じである。工程３００に見られるように、補助制御装置１１０がセーフィングモード１１２で作動しているとき、補助制御装置１１０は、自動車の全体にわたって設置される一連の衝突センサからの信号を監視する（図示せず）。そして、ＭＣＵ１２０は、一連の衝突センサからの受信信号を監視するために衝突アルゴリズム１２２を利用する。当該一連のセンサは、減速力と、その減速力が生じた１または複数の位置とに関して、ＥＣＵ１００へ情報を中継するよう構成される。

【００３５】

工程３１０、３２０において、ＭＣＵ１２０が衝突センサ信号を受信すると、衝突アルゴリズム１２２は、当該信号がＰＳＤ展開に関する所定のパラメータに適合するか否かを決定する。その間、補助制御装置１１０は同時かつ独立に、本発明の技術分野で知られている方法によって、上記信号が所定のパラメータに適合するか否かを確認する。所定の要件が満たされない場合は、ＰＳＤは展開せず、ＭＣＵ１２０は、衝突センサ信号の監視を続ける。

【００３６】

工程３３０、３４０に見られるように、衝突信号が展開のための所定のパラメータに適合することをＭＣＵ１２０衝突アルゴリズムが判定し、また、衝突信号が展開のための所定のパラメータに適合することを補助制御装置１１０が独自に確認した場合、ＭＣＵ１２０は、ＡＮＤゲート１８０に展開信号を送信する。補助制御装置１１０が衝突信号を確認すると、補助制御装置１１０は発火し、補助制御装置１１０はＡＮＤゲート１８０に発火信号を送信する。補助制御装置１１０の発火中、ＡＮＤゲート１８０がＭＣＵ１２０から

の展開信号および補助制御装置１１０からの発火信号の両方を受信すると、衝突アルゴリズム１２２により指定された各ＰＳＤに展開信号が送信され、指定された各ＰＳＤが展開する（工程３５０、３６０）。

【００３７】

図４は、図２の工程２８０に示されるスクラップモード１１４を実行するためのフローチャートを示す。補助制御装置１１０は、ＭＣＵ１２０が復号キーを用いて復号した所定信号を受信したときのみ、スクラップモード１１４に入るよう構成される。工程４００に見られるように、補助制御装置１１０がＭＣＵ１２０から復号された所定信号を受信すると、セーフィングモード１１２の衝突アルゴリズム１２２は中断され、補助制御装置１１０は、廃棄キー１４０を受信したときのみ発火可能となる。補助制御装置１１０が一旦スクラップモード１１４に入ると、補助制御装置１１０は、廃棄キー１４０受信以外のいかなる手段を通しても発火不能であることが望ましいことに注目されたい。

【００３８】

工程４１０において、補助制御装置１１０がスクラップモード１１４に入ると、ＭＣＵ１２０は、外部信号ソースからの廃棄信号に関してＣＡＮを監視し続けることが望ましい。ＭＣＵ１２０が外部信号ソースから廃棄信号を受信すると、ＭＣＵ１２０は、補助制御装置１１０に信号を送信し、廃棄シード１３０を要求する（工程４２０）。廃棄シード１３０は、補助制御装置１１０によりパワーサイクル毎に生成され、もしくは所定の時間間隔で生成される乱数であってよい。

【００３９】

工程４３０において、ＭＣＵ１２０は、補助制御装置１１０から廃棄シード１３０を受信し、廃棄シード１３０に基づいた廃棄キー１４０を計算する。ＭＣＵ１２０は、次に、補助制御装置１１０へ廃棄キー１４０を送信し、ＡＮＤゲート１８０に展開信号を送信する（工程４５０、４４０）。廃棄キー１４０は、ユニークな定期的メッセージとしてもよい。展開信号は、工程２６０において復号された実行可能な指示としてよく、もしくは、テスタから受信された廃棄信号に含めてもよい。展開信号および廃棄キー１４０は、シリアル・ペリフェラル・インタフェース（ＳＰＩ）を介して、ＭＣＵから同時に受信されることが望ましい。

【００４０】

補助制御装置１１０が一旦廃棄キー１４０を受信すると、補助制御装置１１０は、ＭＣＵ１２０から受信した廃棄キー１４０が適切か否かを決定する（工程４６０）。もし、廃棄キー１４０が適切でなかった場合、補助制御装置１１０は発火しないままでいて、適切な廃棄キー１４０に関して監視を続ける（工程４６５）。しかし、仮に補助制御装置１１０が適切な廃棄キー１４０を受信したら、補助制御装置１１０は発火し、工程４７０に見られるように、補助制御装置１１０はＡＮＤゲート１８０に発火信号を送信する。

【００４１】

工程４８０、４９０に見られるように、仮に補助制御装置１１０の発火中にＡＮＤゲート１８０がＭＣＵ１２０からの展開信号および補助制御装置１１０からの発火信号の両方を受信すると、外部信号ソースにより要求されたＰＳＤに、展開信号が送信される。補助制御装置１１０がスクラップモード１１４で作動している時は、ＥＣＵ１００は、外部信号ソースからの廃棄信号を受信しても、単一のＰＳＤしか展開できないよう制限されることが望ましいことに注意されたい。しかし、仮に廃棄信号が複数同時の展開を要求する場合は、単一の廃棄信号受信と同時に、複数のＰＳＤを展開させてよい。

【００４２】

図２および図４に関連して述べられた上記工程は、ＭＣＵ１２０が新しい廃棄要求を外部信号ソースから受信する度に繰り返される。さらに、ＭＣＵ１２０は復号キーの適切さを確認することができないため、復号された指示の適切さ、復号された所定信号の適切さ、およびＣＡＮメッセージ（テスタ）を送信する外部信号ソースの適切さは、補助制御装置１１０にスクラップモード１１４をオンにすることを命じる唯一の手段である。このように、補助制御装置１１０が、ＭＣＵ１２０とは独立して発火することにより、偶発の展

開の危険性を最小限にする。

【００４３】

図５は、補助制御装置１１０がスクラップモード１１４で作動する時の、複数の火工的装置の廃棄方法に関するフローチャートを示している。ＥＣＵ１００は、外部信号ソースから受信した廃棄信号ごとに単一のＰＳＤを展開させるよう、制限されている。工程４９０における単一のＰＳＤの展開に続き、補助制御装置１１０は、工程５１０において一時的にオフにされる。補助制御装置１１０は、補助制御装置１１０に不適切な信号（たとえば適切な展開キー以外の信号）を送信することによりオフにしてよい。補助制御装置１１０が一時的にオフにされたあと、ＭＣＵ１２０は、スクラップ状態が終了したか否かを監視する。スクラップ状態の終了となる状態の例には、ＥＣＵ１００のリセット、ＥＣＵ１００および外部信号ソース間の通信の喪失、もしくは、パワーの喪失が含まれる。スクラップ状態が終了した場合、工程５３０に見られるように、補助制御装置１１０はセーフィングモード１１２に設定される。そして、復号キー、およびＲＡＭに保存された復号された実行可能な指示は破棄してよい。補助制御装置１１０が一旦セーフィングモード１１２に設定されると、補助制御装置１１０は、図２および図４に関連して上述した工程による以外、スクラップモードに設定不能であることが望ましい。

【００４４】

しかし、スクラップ状態が終了していない場合、ＭＣＵ１２０は、テスタからの有効な廃棄信号の監視を続ける（工程５４０）。有効な廃棄信号をＭＣＵ１２０が受信した場合には、工程４１０～４９０において上述したように、補助制御装置１１０は発火し、次のＰＳＤが展開する。この工程は、展開していないすべてのＰＳＤが廃棄されるまで繰り返してよい。

【００４５】

図６は、補助制御装置１１０の実施形態に関する論理略図を示している。上述したように、当初、補助制御装置１１０はセーフィングモード１１２で作動する。所定のメッセージを受信すると同時に、補助制御装置１１０はスクラップモード１１４に入る。スクラップモード１１４は、発火（セーフィング）がオフにされる初期値を有する。補助制御装置１１０が適切でユニークな定期的メッセージ（廃棄キー１４０）を受信すると、発火がオンになる。補助制御装置１１０が不適切でユニークなメッセージ（たとえば不適切な廃棄キー１４０）を受信した場合、もしくは、補助制御装置１１０の発火中に補助制御装置１１０が何らメッセージを受信しなかった場合、発火はオフにされる。最終的には、補助制御装置がリセット命令を受信した場合、補助制御装置１１０は、その初期状態に戻り、セーフィングモード１１２がオンになる。

【００４６】

図７は、補助制御装置１１０およびＭＣＵ１２０のタイミング機能を示すタイミング略図であり、図５に関して上述したように、スクラップモード１１４で複数のＰＳＤを順次展開させる時のものである。時刻t_1において、テスタから送られた新しい廃棄要求信号が、ＭＣＵ１２０によって受信される。ＭＣＵ１２０は、廃棄キー１４０を補助制御装置１１０に送信する。補助制御装置１１０は、補助制御装置１１０を発火させることにより、時刻t_2～t_5間のセーフィングウィンドウをオンにする。セーフィングウィンドウは、時刻t_2～t_3間の発火リード時間を含み、これは、例えば５ミリ秒としてよく、これに限られない。また、セーフィングウィンドウは、時刻t_4～t_5間の発火ラグ時間を含み、これは、例えばおよそ２ミリ秒からおよそ３ミリ秒としてよく、これに限られない。時刻t_3～t_4間のＰＳＤ展開ウィンドウに代表される展開信号（発火電流時間）が、ＭＣＵ１２０によって、当該セーフィングウィンドウ内のＰＳＤに送信された場合、第１のＰＳＤが廃棄される。時刻t_3～t_4間の展開信号は、例えば２ミリ秒としてよく、これに限られない。

【００４７】

時刻t_5において、不適切なメッセージあるいは不適切な信号を送信することによって、ＭＣＵ１２０は、一時的に補助制御装置１１０の発火をオフにする。そして、ＥＣＵは

、時刻t_6において、テスタからの新しい廃棄要求信号を受信可能である。不適切なキーは、ＭＣＵ１２０から補助制御装置１１０へ送信されたメッセージのデータ要素であってもよい。補助制御装置１１０は、不適切な信号あるいは不適切なメッセージが補助制御装置１１０に送信されたときは、セーフィングモードにリセットせず、単にセーフィングを一時的にオフにするだけであることに注目されたい。新しい廃棄要求が時刻t_6において一旦受信されると、新しい廃棄要求のために上記工程が繰り返される。そして、時刻t_8およびt_9で定義されるＰＳＤ展開ウィンドウを、時刻t_7～t_{10}間のセーフィングウィンドウ内の要求されたＰＳＤに送信する必要がある。しかし、補助制御装置１１０は、不適切な信号あるいは不適切なメッセージを受信すると同時にセーフィングモードにリセットされるように構成してもよいことを理解されたい。

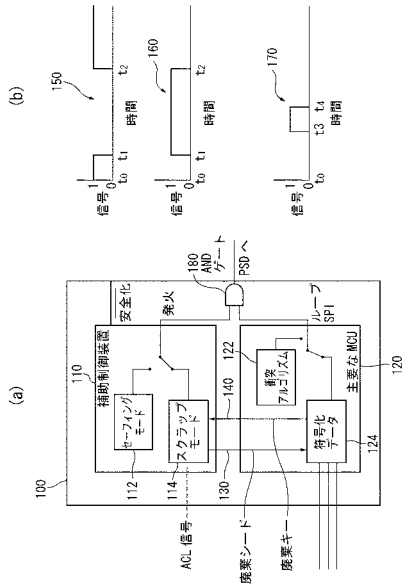
【００４８】

このように、本発明は、ＩＳＯ　２６０２１規約案などの新しい政府規則に準拠する、火工的安全装置の廃棄に関するフェイルセーフ方法を提供する。さらに、本発明は、ＰＳＤを安全に廃棄するために、衝突アルゴリズムおよびセーフィングを作動させるための衝突センサエミュレーションを必要としない。

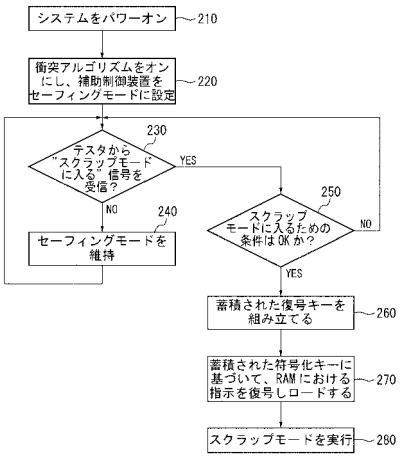
【００４９】

以上、本発明の好ましい実施形態を説明したが、本発明はこれらに限られず、本発明から逸脱しない範囲で改良してよいことを理解されたい。本発明の範囲は、添付の特許請求の範囲によって定義し、特許請求の範囲の意味するところから文言上または均等な意味において想起されるあらゆる工程および装置は、特許請求の範囲に含まれるものとする。さらに、本発明の利点は、必ずしも上述した利点には限られないし、本発明のすべての実施形態において上述の利点のすべてが実現されるとは限らない。

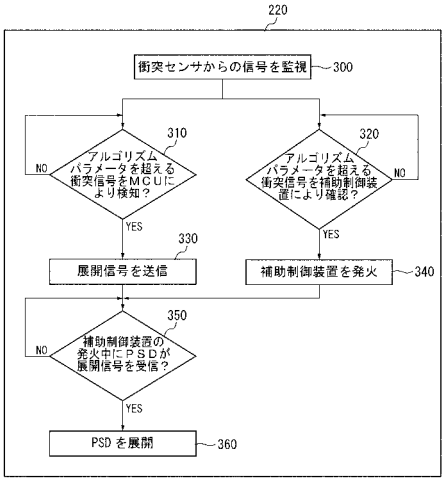
【図１】



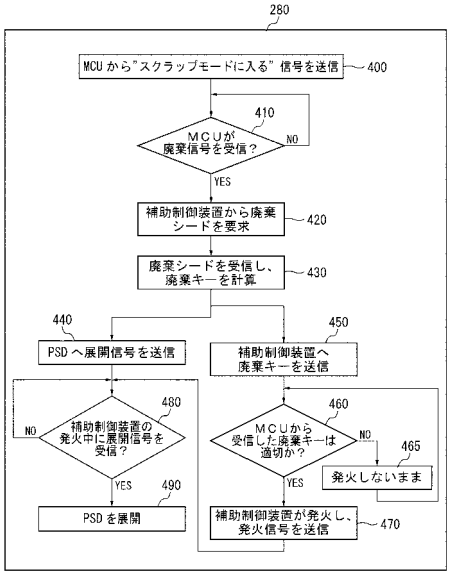
【図２】



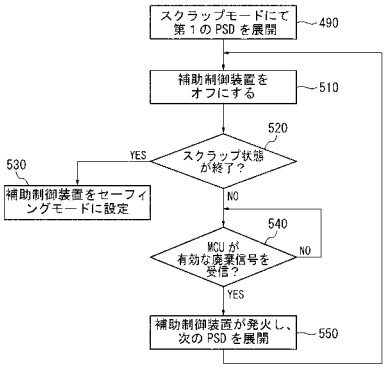
【図３】


220
衝突センサからの信号を監視
300
アルゴリズムパラメータを超える衝突信号をＭＣＵにより検知？
310
NO
YES
展開信号を送信
330
アルゴリズムパラメータを超える衝突信号を補助制御装置により確認？
320
NO
YES
補助制御装置を発火
340
補助制御装置の発火中にＰＳＤが展開信号を受信？
350
NO
YES
PSD を展開
360

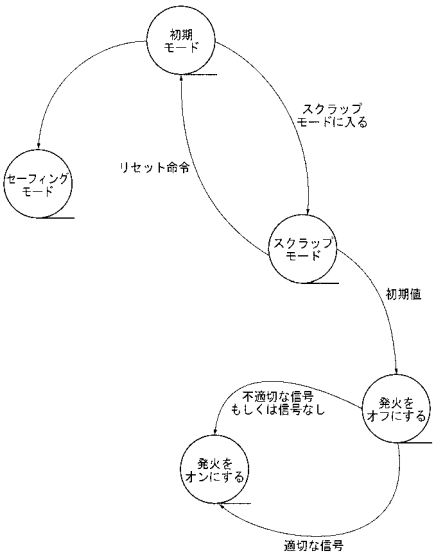
【図４】


280
MCU から”スクラップモードに入る” 信号を送信
400
ＭＣＵが廃棄信号を受信？
410
NO
YES
補助制御装置から廃棄シードを要求
420
廃棄シードを受信し、廃棄キーを計算
430
440
PSD へ展開信号を送信
450
補助制御装置へ廃棄キーを送信
補助制御装置の発火中に展開信号を受信？
480
NO
YES
PSD を展開
490
ＭＣＵから受信した廃棄キーは適切か？
460
NO
YES
465
発火しないまま
補助制御装置が発火し、発火信号を送信
470

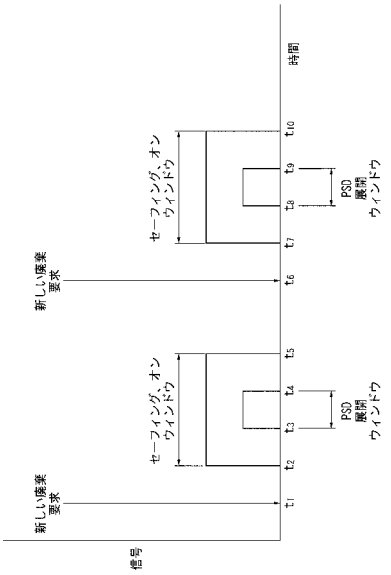
【図５】


スクラップモードにて第１の PSD を展開
490
補助制御装置をオフにする
510
スクラップ状態が終了？
520
YES
NO
補助制御装置をセーフィングモードに設定
530
MCU が有効な廃棄信号を受信？
540
NO
YES
補助制御装置が発火し、次の PSD を展開
550

【図６】


初期モード
スクラップモードに入る
セーフィングモード
リセット命令
スクラップモード
初期値
不適切な信号もしくは信号なし
発火をオフにする
発火をオンにする
適切な信号

【図７】


信号
時間
新しい操業要求
セーフィング・オンウィンドウ
PSD展開ウィンドウ
新しい操業要求
セーフィング・オンウィンドウ
PSD展開ウィンドウ
t1
t2
t3
t4
t5
t6
t7
t8
t9
t10

フロントページの続き

(72)発明者　ベンカトラマン、　ガネシュ　ラム
アメリカ合衆国　ミシガン州　４８１８７、　カントン、　１６４５　ウォルナット　リッジ　サークル
(72)発明者　カールソン、　ヨルゲン　イングバル
スウェーデン国　エスーエスイーー６１６　９１　アビー、　スヨトルプ　ナクナ
(72)発明者　ボラン、　コーム
アメリカ合衆国　ミシガン州　４８３７４、　ノヴィ、　２５７７３　コディ　レーン

審査官　関　裕治朗

(56)参考文献　特開平１１－２９００３（ＪＰ，Ａ）
特開平８－８０８０１（ＪＰ，Ａ）
特開２００６－１５９２２（ＪＰ，Ａ）
特開２００５－８１８７４（ＪＰ，Ａ）
特開２００４－２４９８０８（ＪＰ，Ａ）
特開２００１－５５１０３（ＪＰ，Ａ）
特開平１１－３０１３９５（ＪＰ，Ａ）
特開平１１－３０１３８７（ＪＰ，Ａ）
特開平９－３２３６１５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｂ６０Ｒ　２１／２６４
Ｂ６０Ｒ　２１／０１