汎用端末を用いた保安用途向け接点入出力システムの構成手法

祇園　昭宏*　　福田　光芳**　　中澤　幸弘***

Configuration Method of Relay Input-Output System for a Safety-related Application Using General Purpose Devices

Akihiro GION　　Mitsuyoshi FUKUDA　　Yukihiro NAKAZAWA

In recent years, inexpensive single-board computers with input/output functions and arithmetic functions, such as Raspberry Pi, have been used for various purposes. Condition monitoring and remote control can be mentioned as one of its uses. However, it is very important to ensure safety when applying single-board computers, for example, to safety related equipment. This paper introduces a safety assurance method using pseudo-random numbers and encryption technology to configure a relay-based input/output system with a general-purpose device.

キーワード：汎用端末，信号保安，遠隔監視，フェイルセーフ

1．はじめに

近年，Raspberry Pi に代表される入出力機能や演算機能を備えた安価なボードコンピュータが入手可能になったことや Wi-Fi などの普及により，汎用端末と安価な通信手段を組み合わせたシステムが様々な用途で提案されている。その用途の一つとして状態監視・遠隔制御が挙げられるが，保安に関わる用途への適用では安全性を確保することが重要である。また，汎用端末や公衆無線の利用においては，サイバーセキュリティの観点でも安全を確保することが求められる。本稿では，保安用途への汎用モバイル端末の適用手法[1)]を発展させて，汎用端末により接点入出力システムを構成するための，疑似乱数と暗号化技術を用いた安全性確保手法について報告する。

2．保安に関わる用途における入出力の課題

2.1　検討システムの構成

保安用途の入出力装置として，電子連動装置の現場装置との入出力装置である電子端末[2)3)]が挙げられる。電子連動装置の装置構成を図 1 に示す。電子端末は，連動論理部からの指示により現場装置を制御するとともに，現場装置の状態を取得して連動論理部に表示（通知）する。ここでは，電子端末を Arduino や Raspberry Pi などのボードコンピュータ（汎用端末）に，連動論理部と電子端末間の伝送を汎用の伝送装置と公衆無線にそれぞれ置き換えたシステムについて検討を行った。

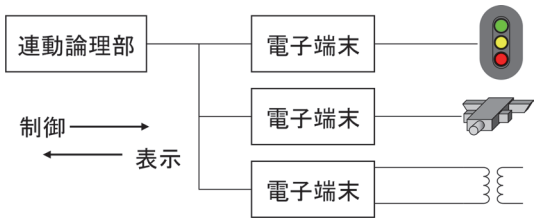


図 1　電子連動装置の構成

2.2　電子端末の安全要件

電子端末の安全要件は，対象となる現場装置の危険な状態を安全と誤認しないこと，制御出力の安全を確保することの 2 点であり，①入出力の故障対策，②健全性確認手法，③故障時の安全側固定の 3 つの原則によって実現している。電子端末の安全確保の考え方について以下に示す。また，各要件への対応を表 1 に示す。

2.2.1　入力

入力については，一般に信号用リレーの落下状態が安全側状態，扛上状態が危険側状態となるため，入力回路の故障によりリレー状態を扛上状態と誤認するリスクが十分に低いことを安全確保の方針としている。

入力回路の例を図 2(a) に示す。リレー状態の入力においては扛上状態の誤認が不安全事象となる。ここでは，フォトカプラが短絡故障した場合に扛上状態の誤認が想定されることから，照査パルス信号でゲートを制御することによりフォトカプラの状態を周期的に変化させて短絡故障を検知することで入力回路の健全性を診断する。具体的には，入力が照査パルスに対応して変化する場合を扛上状態として採用し，不一致の場合は安全側状態と認識する。また，一つのリレーについて N/R の 2 接点を監視する冗長化を行う。

2.2.2　出力

出力については，一般に出力リレーの動作が危険側状

＊　　情報通信技術研究部　通信ネットワーク研究室
＊＊　　情報通信技術研究部
＊＊＊　旧信号・情報技術研究部　列車制御研究室（現　東海旅客鉄道株式会社）

態，落下が安全側状態となるため，出力リレーの制御において出力回路の故障により不正動作となるリスクが十分に低いことを安全確保の方針としている。

出力回路の例を図 2(b) に示す。出力リレーの制御は，フェイルセーフドライバを介して行う。フェイルセーフドライバは，制御ユニットより規定の交番信号が入力された場合に出力する回路であり，さらにリレー出力のフィードバック入力を照査（フィードバック診断）し，異常を検知した場合に交番信号の停止と半導体リレー（Solid Stare Relay: SSR）の制御により出力リレーを落下させ，安全側固定する構成としている。

2.2.3　伝送

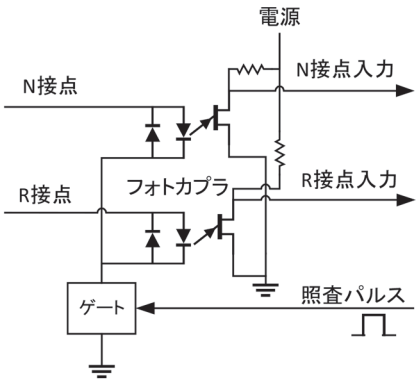
連動論理部と電子端末間でフェイルセーフ通信を行う。通信手順は，連動論理部からのポーリングに電子端末が応答することによる。フェイルセーフ装置である論理部と電子端末が，それぞれ電文の伝送誤りと伝送途絶の検出，異常検出時の安全側制御を行う。伝送誤りの情報は破棄し，伝送途絶時に連動論理部は状態認識を落下側，電子端末は出力を行わないことで安全を確保する。連動論理部と電子端末間の伝送路は信頼できるネットワークを前提とし，自営の有線伝送路を用いる。

2.2.4　処理

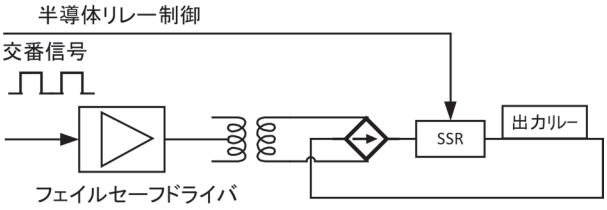
照査パルス診断，フィードバック診断などの電子端末に割り当てられた処理について，系間照合を行い，不一致となる場合は動作を停止する。交番信号を停止するため出力も安全側となる。また，動作停止時は伝送途絶となるため，連動論理部が入力を安全側状態で認識する。入力，出力，伝送についても同様に系間照合を行い，安全を確保する。

表１　入出力の安全要件

	入力	出力
故障対策	照査ﾊﾟﾙｽ診断，N/R 監視	交番信号とﾌｨｰﾄﾞﾊﾞｯｸ診断
故障対策の健全性	フェイルセーフ処理部が故障診断することで健全性確保	
安全固定	異常時は落下と認識	強制的に落下状態とする



(a) 入力回路



(b) 出力回路

図２　電子端末の入出力

2.3　汎用端末適用の課題

ボードコンピュータは処理，入出力，伝送の機能を持つ点では，電子端末と同様である。入出力の故障対策として，照査パルス診断やフィードバック診断を適用した場合も，処理部が非フェイルセーフであるため対策の健全性を保証できない。また，故障時に入出力を安全側に固定する仕組みを装置単体では有しておらず，入力回路の故障，出力回路の故障により不安全事象に至る可能性がある。

セキュリティの観点では，図 3 の階層モデルで示すように，汎用端末，伝送装置，公衆回線のうち信頼できる箇所は汎用端末のユーザーアプリケーション部分のみであり，それ以外の箇所において，なりすましや改ざん，途絶などのサイバー攻撃が想定される。

汎用端末の適用にあたっては，これらのリスクについてコストメリットを損なわずに解決することが課題となる。また，システムの保守や更新が，汎用端末の短い製品寿命に制約されないことも求められる。

3．汎用端末を適用するための安全要件

3.1　安全要件の拡張

入出力に関する不安全事象である，入力情報の危険側誤認と危険側の誤出力について，汎用端末では電子端末のような装置単位での安全確保が困難である。そこで，汎用端末を用いたシステムで安全を確保するよう，安全要件の拡張を行った。

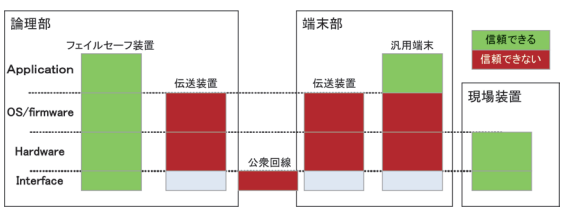


図３　検討システムの階層モデル

3.1.1　入力要件

入力情報について，危険側の情報を定義する。装置の入力と処理，伝送の誤りを検出する方法を定義し，危険側の見逃し誤りのリスクを定量化し，許容できる確率以下となることを示すことを要件とした。

3.1.2　出力要件

出力情報について，危険側情報を定義する。装置の単一故障が発生しても危険側出力が出力されない構成，または誤りを検知して安全側に固定する方法を具備し，危険側の誤出力のリスクを定量化し，許容できる確率以下となることを示すことを要件とした。

3.1.3　電子端末の要件への対応

電子端末の拡張した安全要件への対応を表 2 に示す。拡張した安全要件のもとでも既存の電子端末は要件を満たしている。なお，電子端末では，故障により出力リレーが誤動作してもフィードバックにより検知して，出力リレーの動作前に安全側固定することで，システムとしては誤出力させない構成となっている。これは，機能安全に関する国際規格 IEC 62425 における監視によるフェイルセーフティに相当する。具体的な要件として，入力情報について危険側の情報を定義することと，装置の入力と処理，および伝送の誤りを検出する方法を定義し，危険側の見逃し誤りのリスクを定量化し，許容できる確率以下となることを示すこととした。

3.2　セキュリティ要件

セキュリティ確保の基本方針をシステムの信頼できる箇所を明確化するとともに，信頼できない箇所におけるサイバー攻撃を信頼できる箇所において検証することと定めた。セキュリティの要件として，計算量的安全性などで定量化するとともに検証機能の健全性を確保することを定めた。

4．汎用端末による入出力システムの構成手法

安全とセキュリティの課題を解決し，コストやシステム保守の要求に対応するため，フェイルセーフ装置に検証を，汎用端末に処理を割り当てる構成手法を開発した。

4.1　フィードバック診断手法

フィードバック診断の手法として，信号用リレーの入出力に用いる汎用端末を出力端末と応答端末の二台構成として，応答端末の出力を監視することにより，リレー状態の危険側誤認と危険側誤出力を防ぐ。この場合，汎用端末にハードウェアの改造は必要なく，機能レベルの互換性を持たせることで置換えが可能であることからコストやシステム保守の要求に対応する。

4.1.1　入力

図 4 に示すように，①中央装置は監視指示として乱数生成情報を出力端末である端末 #1 に送る。②端末 #1 は乱数生成情報に基づく乱数を生成して，応答端末である端末 #2 にリレーR_0を介して伝送する。③端末 #2 は乱数を取得して中央装置に応答する。中央装置は，応答された乱数の照合を行い，リレー状態を認識する。

4.1.2　出力

図 5 に示すように，出力リレーR_0を 2 台の端末（端末 #1，端末 #2）が独立して制御する 2 つのリレー（端末 #1 で制御する R_A，端末 #2 で制御する R_B）の AND 条件で動作するように構成する。端末 #1 からの出力 R_A を端末 #2 でフィードバック診断した後に，端末 #2 からの出力 R_B を制御する二段階制御とすることにより，端末故障が発生した場合の不正な出力を防ぐ。

4.2　セキュリティ手法の適用

セキュリティ上の脅威としては，電文の改ざんや装置のなりすまし，DoS 攻撃（Denial-of-service attack）など

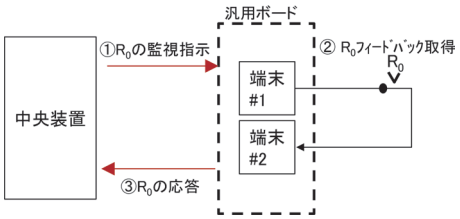


図４　入力制御

表２　電子端末の拡張した安全要件への対応

	安全要件	電子端末での対応
入力	危険側となる情報の定義	扛上接点の誤認
	故障の識別と安全側固定	照査パルス診断をフェイルセーフ処理部が実施，故障時は落下側と認識
	見逃し誤りが許容値以下	フェイルセーフ処理部の両系同時故障の確率が低いことによる
出力	危険側となる情報の定義	出力リレーの不正動作
	単一故障に対する対策	フェイルセーフドライバによる制御
	誤りの識別	フィードバック診断をフェイルセーフ処理部が実施，故障時はリレーを強制落下
	見逃し誤りが許容値以下	フェイルセーフ処理部の両系同時故障の確率が低いことによる

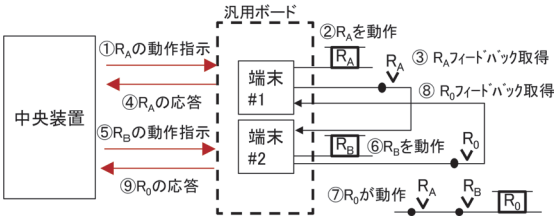


図５　出力制御

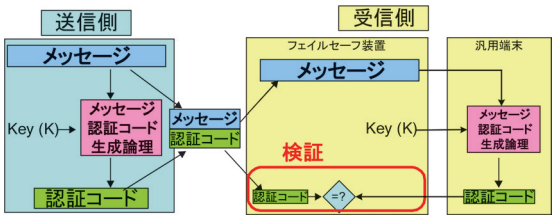


図６　認証コードの検証フロー

のサイバー攻撃が想定される。端末を介した入出力において，危険側となりうるサイバー攻撃は，端末へのなりすましと改ざんであることから，電子署名による端末の真正性（Authenticity）の検証，メッセージ認証コードによる完全性（Integrity）の検証を行う。セキュリティ要件への対応として，米国国立標準技術研究所（NIST）のセキュリティ基準に関するガイドライン[4]にて，2031 年以降も利用可能な方式とされる HMAC-SHA256 を適用する。検証機能の健全性は，図 6 に示すように汎用端末とフェイルセーフ装置で暗号処理と検証を分離することで確保する。暗号技術の陳腐化に際してもフェイルセーフ装置の役割は汎用端末のフロントエンドと認証コードのマッチング検証であるため改修は必要なく，汎用端末に適用する暗号処理の高度化により対応可能である。

5．軌道回路監視システムの試作

5.1　システムの概要

信号用リレーの遠隔監視を保安用途へ適用する例として，中間軌道回路の状態監視システムを検討した。中間軌道回路の状態を列車接近警報システムに活用することで作業の安全性向上が期待されるが，軌道リレーは広範囲に点在するため，電子端末による構成は導入コストが大きく困難である。そこで，図 7 に示すように，軌道回路の監視に汎用端末を，汎用端末と中央装置の伝送に公衆無線を用いて監視システムを構成する。

5.2　試作したシステムの構成

試作システムは，列車走行を模擬して列車の在線位置に応じたリレー制御を行う列車走行模擬装置と，4.1.1 節の入力制御の構成により軌道リレーの状態を監視する軌道回路監視装置より構成する。システムの構成を図 8

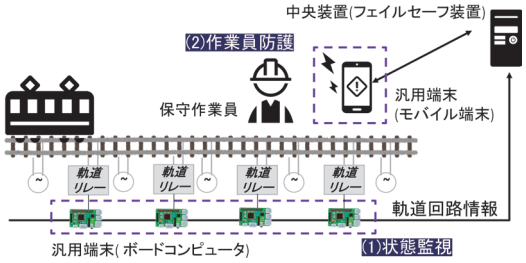


図７　軌道回路監視システムの構成

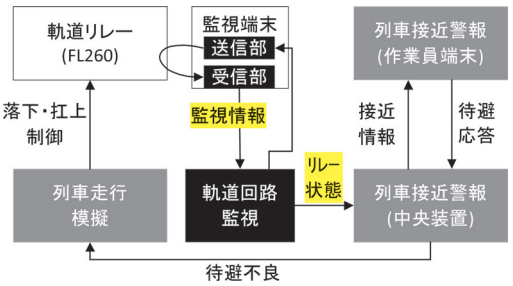


図８　試作システムの構成

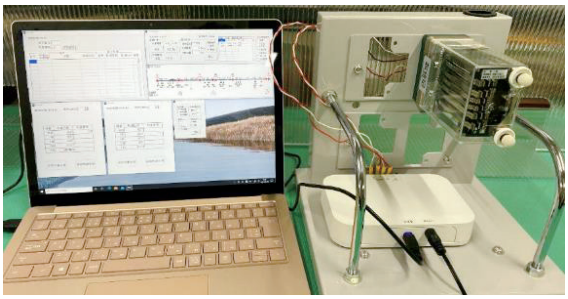


図９　列車走行模擬装置と軌道回路監視装置

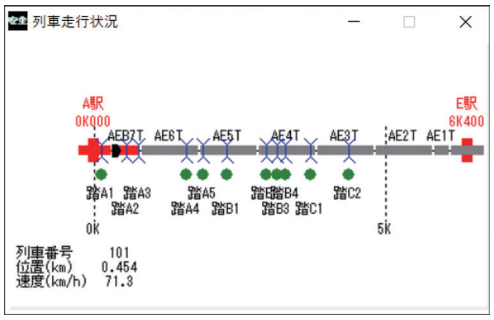


図 10　列車走行模擬装置の画面例

に，試作した装置を図 9 に，列車走行模擬装置の画面を図 10 にそれぞれ示す。また，試作システムの安全要件への対応を表 3 に，軌道リレー監視に用いたボードコンピュータ，ESP32[5]の諸元を表 4 に示す。

軌道回路システムにより得られたリレー状態情報の保安用途への活用として，汎用モバイル端末の保安用途適用の検討[6]で試作したフィードバック型列車接近警報の列車位置情報としての利用について検証を行った。

表３　試作システムの安全要件への対応

	安全要件	試作システムでの対応
入力	危険側となる情報の定義	扛上接点の誤認
	故障の識別と安全側固定	汎用装置が応答する乱数の照査。照査不一致，途絶を落下と認識
	見逃し誤りが許容値以下	フェイルセーフ処理部の故障，乱数の偶発一致確率が低い（乱数長 32bit：2.3×10^{-10}，64bit：5.4×10^{-20}）
出力	危険側となる情報の定義	出力リレーの不正動作
	単一故障に対する対策	二段階制御
	誤りの識別	フェイルセーフ処理部による診断。故障時は出力制御を停止
	見逃し誤りが許容値以下	フェイルセーフ処理部の故障，乱数の偶発一致確率が低い
セキュリティ	計算量的安全性	HMAC-SHA256 のセキュリティ強度により確保
	検証機能の健全性	フェイルセーフ処理部が検証することにより確保

表４　ESP32 の性能諸元

機能		諸元
処理	CPU	Xtensa LX6 240MHz（600DMIPS）
	RAM	520KB（SRAM）
	ROM	4MB
IO	入力	Digital 21 接点（共用）
	出力	
伝送		SPI 4，I2S 2，I2C 2，UART 3 802.11b/g/n，Bluetooth

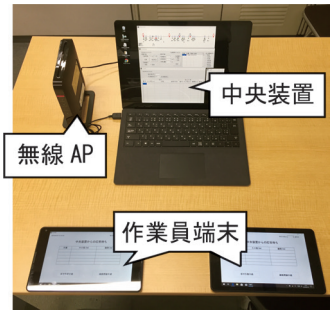


図 11　列車接近警報システムの装置構成

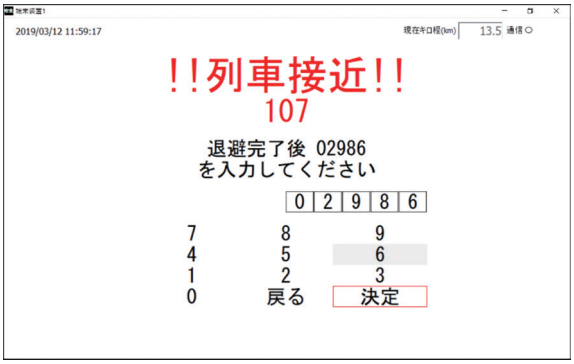


図 12　作業員端末の画面表示（接近時）

試作システムは，列車接近警報の条件となる軌道回路を模擬するとともに，列車接近警報システムの中央装置にリレー状態を通知する設定とした。列車接近警報システムは，試作システムにおける軌道回路の落下により中央装置より作業員端末に警報を指示し，作業員端末からの待避完了を取得出来ない場合に中央装置が列車走行模擬装置に対して待避不良を通知する構成とした。列車接近警報システムの構成を図 11 に，作業員端末の画面を図 12 に示す。

5.3　機能検証結果

軌道回路監視装置について，装置故障とサイバー攻撃を想定した機能検証を実施した。検証項目と結果を表 5 に示す。検証の結果，入力，処理，出力，伝送，セキュリティのすべての試験項目について安全が確保できることを確認した。本機能検証の結果より，保安システムの入出力用途に汎用端末と公衆無線を適用できる見通しを得た。

6．まとめ

汎用端末と公衆無線を用いた入出力監視システムを保安に関わる用途へ適用するための検討として，電子連動装置の入出力装置である電子端末の安全要件の抽出とセキュリティ要件の整理を行った。そして，安全とセキュリティの課題，およびコストと保守や更新の要求に対応するシステム構成手法として，処理と検証の分離によるフィードバック診断とセキュリティ診断手法を開発し，中間軌道回路の監視用途に提案手法を適用したシステムを試作した。

試作システムを用いた機能検証により，装置故障，伝送異常，サイバー攻撃に対して安全を確保できること，また，安全要件とセキュリティ要件を満たすことを確認できたことから，汎用端末と公衆無線を，保安システムへの情報取り込みに適用できる見通しを得た。

今後は，軌道回路監視以外の用途への活用について構成手法と検証手法をとりまとめるほか，フェイルセーフ

表５　機能試験項目と結果

機能	故障モード	結果
入力機能	応答端末の入力誤り	フェイルセーフ部で乱数の不一致を判定
	応答端末の入力停止	無検知状態となり落下側と認識
処理機能	出力端末の乱数誤り	フェイルセーフ部で乱数の不一致を判定
	応答端末の署名誤り	フェイルセーフ部で改ざんとして検出
出力機能	出力端末の誤出力	フェイルセーフ部で乱数の不一致を判定
	出力端末の出力停止	無検知状態となり，落下側と認識
伝送機能	乱数生成情報誤り	検定符号により出力端末が誤りを検知 （見逃し誤りの場合も乱数の不一致を判定可能）
	応答端末の電文誤り	検定符号によりフェイルセーフ部が誤りを検知
	伝送途絶	乱数が更新されない，応答端末の停止として状態を落下側と認識
	伝送遅延	伝送遅延　　途絶判定により落下側と認識
セキュリティ	再送攻撃	通番と乱数変更により異常電文として検知，破棄
	暗号鍵の不一致	署名の検定誤りにより異常電文として検知，破棄
	DoS 攻撃	途絶と同様に落下側と認識

処理部によらない照合の健全性確保について検討を行う予定である。

文　献

1）祇園昭宏，岩田浩司：安全関連系端末の安全要件および適用事例についての検討，第 27 回春季信頼性シンポジウム発表報文集，6-2，pp.127-130，2019

2）川口剛，酒巻正男：電子連動装置（5）電子端末，鉄道と電気技術，Vol.4，No.12，pp.57-62，1993

3）関貫造：電子連動装置（7）電子端末 K 形，鉄道と電気技術，Vol.5，No.2，pp.65-69，1994

4）National Institute of Standards and Technology：Recommendation for Key Management: Part 1 - General, SP 800-57 Part 1 Rev. 5，2020.

5）ESP32 マイコンドキュメント：https://www.espressif.com/en/support/documents/technical-documents
（参照日：2022 年 3 月 20 日）

6）祇園昭宏，岩田浩司：高い安全性を要する用途への汎用モバイル端末の適用，鉄道総研報告，Vol.33，No.7，pp.35-40，2019