鉄 道 総 研 報 告

特集：信号通信技術

高い安全性を要する用途への汎用モバイル端末の適用

祇園　昭宏*　　岩田　浩司*

Application of General-Purpose Mobile Devices for High Safety Required Use

Akihiro GION　　Koji IWATA

We organized a method and requirements for using a general-purpose mobile devices for safety related applications. First, we classified applications of mobile devices in maintenance work into three types and defined hazards. Secondly, we extracted hazards of input, output and processing functions, arranged safety requirements, and proposed a system configuration method and feedback diagnosis method. We defined a feedback type approaching train alarm that applies proposal methods and confirmed the prototype system ensuring safety when the terminal fails or the handling error.

キーワード：汎用モバイル端末，安全関連系，保守作業，商用オフザシェルフ

1．はじめに

近年の情報通信技術の発達と端末装置の低廉化により，多種多様な情報をあらゆる場所で容易にやり取りすることが可能となりつつある。鉄道信号分野においても，就業人口の減少に対応した業務の効率化と省力化，また，さらなる安全性向上による労働環境の改善のため，スマートフォン等の汎用モバイル端末を保守作業に活用するニーズが存在する[1) 2) 3)]。しかし，汎用モバイル端末は非フェールセーフ構成装置であり，高い安全性が要求される用途へそのまま適用することが困難であった。また，端末装置をフェールセーフ構成とすることは端末の調達コストを増大させるとともに継続的な供給を困難とし，システムの寿命を制約する要因となると懸念される。

そこで，高い安全性を要する用途への汎用モバイル端末の適用についてシステムの構成手法を定めるとともに，ハードウェア的な改造をすることなく汎用の端末装置を活用して安全を担保するための考え方・要件について整理を行った[4)]。また，その適用例として，端末装置の健全性を中央装置にて常時確認するフィードバック型構成を特徴とする列車接近警報システムについて試作を行ったので報告する。

2．保守作業における端末の用途と課題

保守作業における作業員向け端末の用途は，文献1から文献3において列車情報表示(TID)メンテナンス管理，線路閉鎖手続き・進路設定，列車接近警報が示されている。これらの用途について，安全に関わらない用途，別装置が安全を確保する用途，端末が安全を確保する用途の3種別に整理した結果を表1に示す。

これらの用途において，端末はシステムと取扱者とのマンマシンインターフェース装置となる。汎用モバイル端末の構成[5)]は，図1に示すように，フェールセーフコンピュータの構成となっていないため，高い安全性が要求される用途への適用にあたっては，画面または音声での入出力機能，通信機能，処理機能のそれぞれについて，故障検知と安全側制御が課題となる。また，端末装置の故障について取扱者が注意する必要があり，安全に対して取扱者の負担が大きいという課題がある。

信号保安装置に用いるフェールセーフ構成機器は，専用品・特注品であるため高価だが提供期間は比較的長い（10～15年）のに対して，汎用モバイル端末は汎用品のため安価だが提供期間は短い（2年程度）という特徴があり，システムを構築する上ではシステム寿命の確保も重要な課題である。

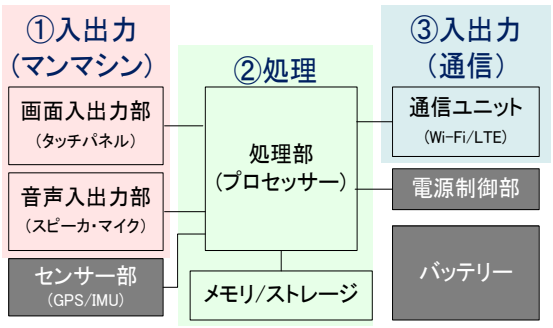

図1　汎用モバイル端末の構成

＊　信号・情報技術研究部　列車制御研究室

表１　端末装置の用途と分類

レベル	用途	入力	出力	処理
安全に関わらない（レベル 0）	TID [1]	なし	在線情報表示	なし
	メンテナンス管理 [1]	設備情報	設備情報表示	なし
別装置が安全を確保（レベル 1）	線路閉鎖手続 [2]	設定・解除要求	設定・解除表示	なし
	進路設定 [2]	設定・解除要求	設定・解除表示	なし
端末が安全を確保（レベル 2）	列車接近警報 [3]	端末位置	在線情報表示 警報表示・警報音	警報判定

３．安全が要求されるシステムの構成手法

3.1　システム構成手法

システム構成における安全要件を，「システムの安全上のリスクを，端末装置の故障や，取扱者の単純な誤りに対して許容できる程度にまで低減するために，端末の入出力および処理と，取扱者の確認を定めること」と定義し，システムの安全要件を満たすシステムの構成手法として，図 2 に示すフローを提案する。

提案するフローでは，まずシステムの安全分析フェーズとして取扱者を含めた装置の特定と，機能・入出力の抽出をおこない，事前安全性解析を実施する。

次に，安全要件適用フェーズとして安全分析フェーズで抽出したシステムの危険側事象と，その要因となる機能・入出力を特定し，端末装置と取扱者の確認に関連する項目について機能要件を適用し，誤って危険側の状態とならないように構成する。

表 2 に，システムにおける安全要件を示す。

提案フローにおいては，汎用モバイル端末を入出力と処理の単位と定義するため，システムは疎結合となる。異なる端末を使用する場合も，機能的な互換性を確保することにより，汎用モバイル端末の更新･保守を可能とし，システムの寿命を確保する。また，誤って危険側となることの回避を検討対象としているが，アベイラビリティの観点で望ましくない状態や情報についても含めてよい。

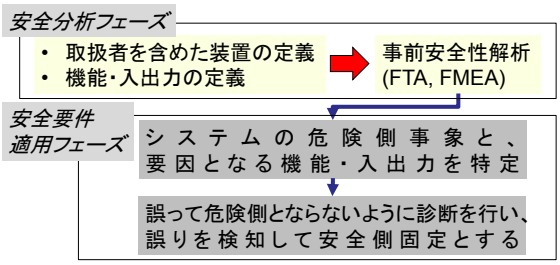

図２　提案するシステム構成フロー

3.2　機能の構成手法

3.2.1　機能の安全要件

汎用モバイル端末の，入出力と処理の各機能の安全要件として，安全確保のために必要となる故障検知と安全側制御に関する基本方針を示す。

(1) 入力機能
・画面入力

表２　システムにおける安全要件

		安全要件
システム		システムの安全上のリスクが，端末装置の故障や，取扱者の単純な誤りに対して許容できる程度にまで低減されていること
		システムの安全分析に基づき，システムで取り扱う情報や処理の結果について安全側と危険側の状態を割り当て，誤って危険側の状態とならないような構成とすること
端末装置	概要	入出力・処理の誤りによるシステムの安全上のリスクが許容できる程度にまで低減されていること
	入出力	情報の危険側の割り当てを行い，誤って危険側とならないようにすること。誤りを検知して安全側固定とすること
	処理	処理の結果について危険側の割り当てを行い，誤って危険側とならないようにすること。誤りを検知して安全側固定とすること
取扱者	概要	単純な入力誤り，確認誤りによるシステムの安全上のリスクが許容できる程度にまで低減されていること
	入力	入力値の誤りを取扱者とシステムで確認する仕組みをもつこと
	確認	取扱者の確認誤りについて検知する仕組みをもつこと

① 故障検知
端末装置の入力部に対する故障診断を行い，正常に機能することを確認する。
② 安全側制御
故障を検知した場合は，使用する入力部に応じた安全側制御を行う。
・SI（シリアル入力）
① 故障検知
端末装置の SI 部に対する故障診断を行い，正常に機能することを確認する。
② 安全側制御
故障を検知した場合は，使用する SO（シリアル出力）に応じた安全側制御を行う。

(2) 出力機能
・画面出力
① 故障検知
端末装置の画面出力部に対する故障診断を行い，正常に機能することを確認する。
② 安全側制御
出力画面の故障を検知した場合は，使用する画面に応じた安全側制御を行う。
・SO（シリアル出力）
① 故障検知
端末装置の SO 部に対する故障診断を行い，正常に機能することを確認する。
② 安全側制御
故障を検知した場合は，使用する SO に応じた安全側制御を行う。

(3) 処理機能
① 処理誤り頻度の低減
端末装置での処理誤りの発生を極力抑制する構成とする。
② 故障検知
端末装置において発生した処理誤り検知のため，診断を行い処理結果が正しいことを確認する。
③ 安全側制御
端末装置の処理部の故障を検知した場合は，処理部を安全側に制御する。
④ 健全性確認
端末装置が故障した状態のまま，取扱者が作業を継続することを防ぐため，端末の健全性を示す情報を常時出力し，端末装置が故障していることを早期に取扱者が認識できるようにする。

(4) その他
フェールセーフ処理部と安全関連系端末間の伝送誤りを相互に検知するほか，伝送途絶を検知した場合に，使用する用途に応じた安全側制御を行う[6]。

3.2.2 構成手法
(1) 入出力の構成手法
端末の画面および音声入出力の誤りについて安全性を確保するために，出力を入力として取り込み，フェールセーフ構成装置で照合する方法を検討した。画面入出力診断の構成手法を図 3 に，音声入出力診断の構成手法を図 4 に示す。

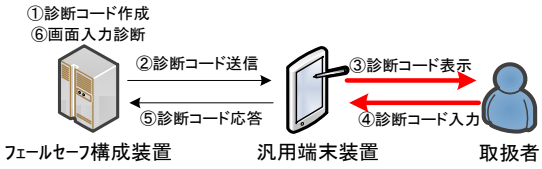

図３　画面入出力診断構成手法

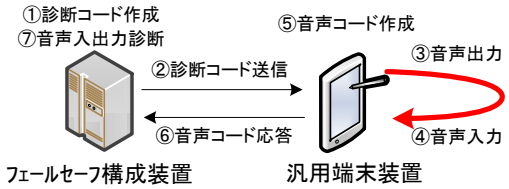

図４　音声入出力診断構成手法

(2) 処理の構成手法
フェールセーフコンピュータでは，複数の CPU で処理を実行し，処理結果を照合することにより処理のフェールセーフ性を確保する。その実装方法として，図 5 に示すようなバス同期式，位相差同期式，プログラム同期式がある。
汎用モバイル端末を用いたシステムで処理と同期と照合の 3 ステップを実装する方法として，ネットワーク上のフェールセーフ処理部で汎用モバイル端末の処理を照

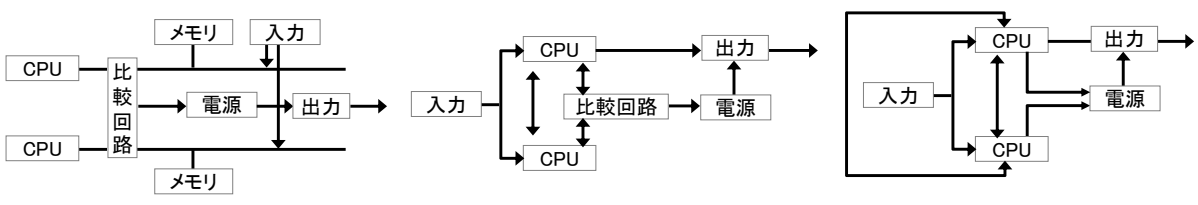

図５　フェールセーフコンピュータの構成手法

合することによりプログラム同期方式を実現する，装置間照合方式を検討した。

端末装置間照合構成は，処理は端末装置で行い，ネットワークを介して処理結果をフェールセーフ処理部で比較照合し，処理と照合結果に基づいて端末装置が出力を行う。概要を図 6 に示す。

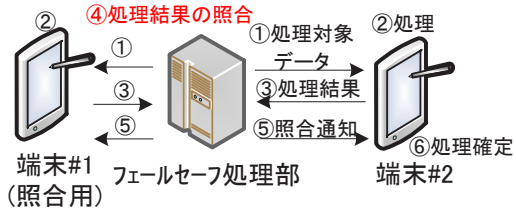

図 6　端末装置間照合構成

4．列車接近警報への適用

列車接近警報について，3.1 節のフローと 3.2 節の機能要件を適用したフィードバック型列車接近警報システムについて述べる。

4.1　列車接近警報の安全関連系要件

列車接近警報のシステムとしての安全要件を抽出する。列車接近警報は，作業箇所への列車接近時に端末が警報出力し，作業員防護をおこなうシステムである。図 7 に示すシステム構成のように，中央装置と端末装置と作業員から構成される。中央装置は列車位置情報を集約して端末装置に配信し，端末装置は作業員の設定した位置情報と中央装置から配信された列車位置情報より列車接近を判定し，列車接近時に警報出力を行う。列車接近警報システムの機能構成図を図 8 に示す。列車接近警報に関する FMEA の例を表 3 に，FTA の例を図 9 に示す。

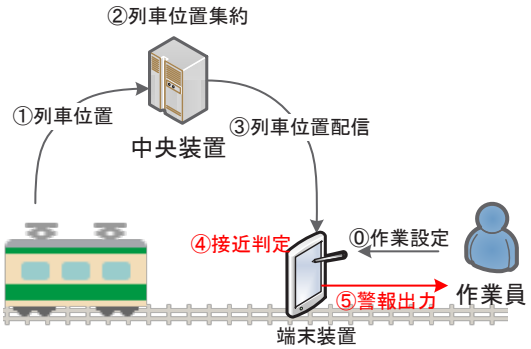

図 7　列車接近警報の装置構成

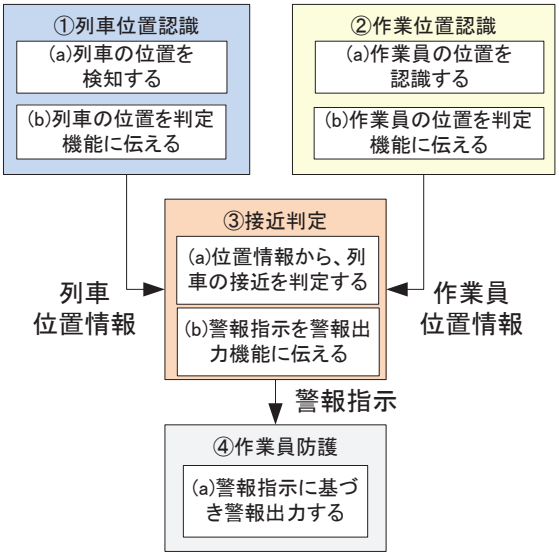

図 8　列車接近警報の機能構成図

FTA 分析より，作業員の待避不良という危険事象について，出力の危険状態である「警報出力しない」事象，警報判定の誤りを構成するうちの処理において「端末が列車接近なしと誤判定する」事象，入力において「誤った作業位置の設定」事象を危険状態として抽出できる。

したがって，安全関連系として構成するための要件として，入出力について「警報出力したこと」「正しい作業位置が設定されたこと」が確認項目として抽出され，処理については「列車接近なしとの判定処理についての照合」が抽出される。

表 3　列車接近警報の FMEA 例（機能レベル）

機能	故障モード	影響	対策の例	対策の効果
列車位置認識	列車検知の抜け	接近判定誤り		—
	列車検知の誤り	接近判定誤り		—
	列車位置情報の受信誤り	接近判定誤り	伝送上の対策	伝送誤りなし
作業員位置認識	位置設定の誤り	接近判定誤り	作業員による確認	作業員位置の誤り低減
接近判定	処理誤り	接近判定誤り		—
警報出力	警報指示の途絶	警報出力故障	途絶検知	故障出力
	スピーカの故障	警報出力故障		—
	音量設定の誤り	警報出力故障		—

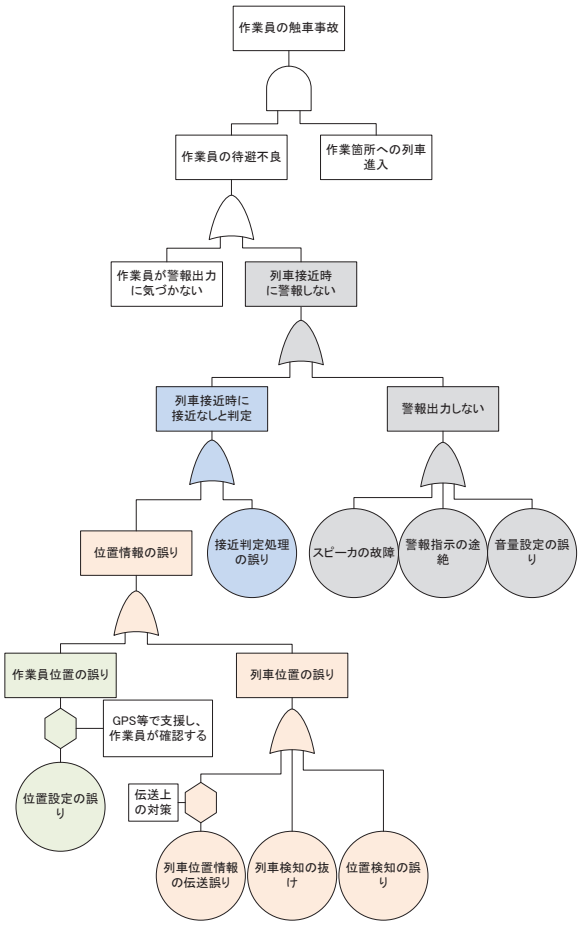

図９　列車接近警報の FTA 例

図 10　作業位置の入力に対する確認

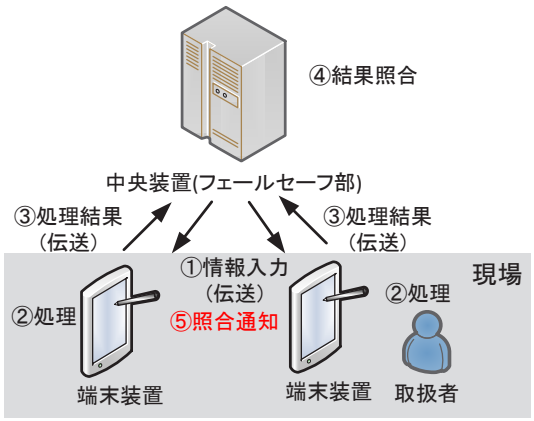

図 11　端末装置間照合による接近判定処理の一致確認

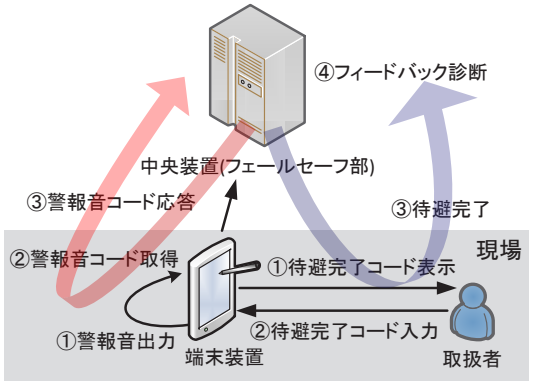

図 12　警報出力と待避確認

4.2　フィードバック型列車接近警報の構成

列車接近警報の安全分析によって抽出した「警報出力したこと」「正しい作業位置が設定されたこと」の入出力確認と，「列車接近なしとの判定処理」の照合を列車接近警報に適用し，さらに作業員の待避不良という危険事象について「待避時の作業員応答がないこと」を確認するフィードバック型列車接近警報システムを定義する。

(1) 作業位置の入力

作業位置の入力においては，図 10 に示すように，入力された作業位置をフェールセーフ部が診断値と共にアンサーバックし，取扱者が表示を確認して診断値を入力するフローとする。入力された作業位置が応答していることを取扱者が確認するフィードバックチェックと，診断部が作成した診断値が取扱者の確認入力によって応答していることを確認するフィードバックチェックにより，取扱者の誤入力と，端末の故障による誤設定を防ぐ。

(2) 接近判定

接近判定においては，図 11 に示すように，同一作業箇所の端末装置が同じ情報入力 (作業位置・列車位置) に対して接近判定処理を行い，フェールセーフ部に結果を応答し，フェールセーフ部で端末装置間の処理結果を照合する。端末装置は，処理結果が「接近なし」の場合はフェールセーフ部からの照合通知により「一致」と確認するまで処理結果を保留し，「接近なし」と誤って判定することを防ぐ。処理結果が「接近あり」の場合や，中央装置からの照合通知が途絶，または「不一致」の場合，端末装置は「接近あり」として警報出力を行う。

(3) 警報出力・待避判定

接近判定処理において，フェールセーフ部は端末装置の警報の有無を把握する。端末装置は，警報出力時に警報音とともに待避完了コードを表示し，フェールセーフ部でこれを照合することによって警報出力と待避判定を行う。概要を図 12 に示す。

警報出力判定においては，端末装置は警報音のフィー

表４　機能試験項目と結果

機能	故障モード	結果
入力機能	取扱者の入力誤り	取扱者の確認入力誤りを中央装置が検知
	警報時の無応答	中央装置で待避不良を検知
	位置情報の途絶 / 誤り	端末装置・中央装置で異常判定
処理機能	接近判定の誤り	中央装置で異常判定
出力機能	警報の未出力	中央装置で待避不良を検知
	接近判定の途絶	端末装置と中央装置で通信の途絶を異常判定
	応答の途絶 / 誤り	中央装置で取扱者の待避不良を検知

ドバック入力で得た警報音コードをフェールセーフ部に送り，フェールセーフ部は警報音コードの一致により音声出力の健全性を把握する。

待避判定においては，端末装置は取扱者の入力で得た待避完了コードをフェールセーフ部に送り，フェールセーフ部は待避完了コードの一致により待避完了を把握する。待避完了コードが途絶等によりフェールセーフ部で得られなかった場合は待避不良とみなし，作業員防護のための措置をとることができる。

4.3　試作と機能検証結果

4.2 節に示したフィードバック型列車接近警報について，実証システムの試作と機能検証を実施した。

試作したシステムの構成を図 13 に，システム機能試験項目と結果を表 4 に示す。

端末装置の故障や伝送異常，取扱者の入力誤りについて，フィードバック診断により中央装置で把握できることを確認した。

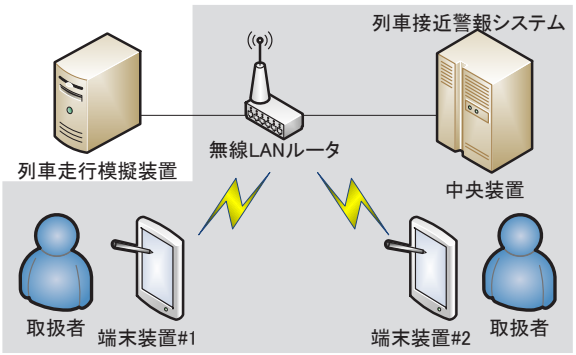

図 13　試作したシステムの装置構成

5．まとめ

汎用のモバイル端末を，安全関連系端末として活用するために必要となる安全担保の考え方や要件の整理を行った。保守作業での汎用のモバイル端末の用途について，安全性確保における課題を抽出するため，安全に関わらない用途，端末以外の装置が安全を確保する用途，端末が安全を確保する用途の 3 つに分類し，危険事象を整理した。また，汎用のモバイル端末の入力，出力，処理の各機能について危険事象を抽出して安全要件を整理し，安全関連系システムの構成手法，各機能の安全を確保するためのフィードバック診断手法を提案した。

列車接近警報について，安全関連系システムの構成手法とフィードバック診断手法を適用したフィードバック型列車接近警報を定義してプロトタイプシステムの試作を行い，端末装置の故障や伝送異常，取扱者の入力誤りに対してフィードバック診断によって異常検知できることを確認した。

今後は，信号保安システムにおける汎用端末の更なる利活用のため，信号リレーの状態監視や遠隔制御の汎用端末による実現について，本研究で得られた知見を活用して研究を行う。

文　献

1）西村佳久：鉄道におけるタブレット端末の活用，鉄道と電気技術 , Vol.26, No.5, pp.3-9，2015
2）下一幸，内田敏博，佐竹渉：線閉・保守作業手続きシステムの開発，JR EAST Technical Review, No.49, pp.49-52, 2014
3）齋藤輝明，大塚勝，佐々木敦：軌道回路のない区間の列車接近警報装置の開発，JR EAST Technical Review, No.49, pp.53-56，2014
4）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 31 回秋季信頼性シンポジウム , 日本信頼性学会，pp.113-116，2018
5）Intel Atom® Processor Z3700 Series：https://www.intel.co.jp/content/www/jp/ja/design/mobile-devices/platforms/bay-trail-cr/overview.html,（参照日 2019 年 3 月 10 日）
6）福田光芳，岩田浩司，菅原宏之，北野隆康，川﨑邦弘：非安全関連装置混在環境における保安情報伝送の評価，鉄道総研報告 Vol30, No.1, pp.29-34，2016