鉄 道 総 研 報 告

特集：信号通信技術

列車制御システムの概念設計段階における安全性確認手法

岩田　浩司*

A Method to Verify Conceptual Design Specifications on Safety Requirements for Train Control Systems

Koji IWATA

High levels of safety are required for train control systems. It is important to apply all required safety measures to the train control systems without any omissions. As recent train control systems require much more functions than before, it is necessary to divide the design phase into the conceptual design phase and the detailed design one, in order to avoid the complexity of systems design. In this paper, we propose the format of safety requirements, which are to be used as a guideline for system design positioned between "safety guidelines for computerized train control and protection systems" and detailed design examples, and a method to verify the specifications of the system requirement phase with this format.

キーワード：列車制御システム , システム安全要求仕様 , 安全性

1．はじめに

列車制御システムは，信号機・転てつ機等の装置を制御することから，高い安全性が要求される。このため，設計段階においてFTA（Fault Tree Analysis），FMEA（Failure Mode and Effects Analysis）などの安全性解析を行い，システムに潜在する不安全事象を可能な限り特定し，フェールセーフを基本とした安全性対策が施される。

列車制御システムでは，構成要素となる各装置内のハードウェアとソフトウェアの安全性・信頼性に加えて，これらを組み合わせた装置ならびに複数装置を接続したシステム全体としての仕様の定義を漏れなく行うことが安全性確保において重要である。よって，システムの確実な動作には，システムライフサイクルの最上流に位置するシステム仕様が大きな役割を担う。

近年，列車制御システムは多機能化しつつあり，このシステムの安全性を確保するためには，ソフトウェアだけでなくハードウェアも含めた列車制御システム全体としての安全性対策を，システムを構成する機能ごとに安全要件として定めて体系的に管理し，また，これらを確実に組み込む仕組みが必要である。これら作業を的確に実施するためには，安全性確認項目を自動的に生成する必要があると考え，列車制御システムの機能に着目した安全要件のフォーマット，ならびにこのフォーマットを活用した安全性確認手法を提案する。以下，提案手法，無線を用いた列車制御システムCARATを一例とした適用結果，ならびに，提案手法を効率的に実施するための安全性確認支援ツールについて述べる。

2．列車制御システムの概要

2.1　近年の列車制御システムの特徴

コンピュータ制御による電子連動装置が導入されて20年以上経過し[1)]，フェールセーフCPUボード（保安装置用フェールセーフ処理ボード。以下，FS-CPUボード）上のソフトウェアで実現される機能は，CPU処理能力の向上とともに，保守性の向上等のため多種類となり，システムは複数の制御モードを有する。また，装置間のネットワーク化，機器の小型化も進み，機器室外の現場に設置される信号機自体も端末化されたネットワーク信号システムも実用化された[2)]。

一方，鉄道のRAMS（信頼性，可用性：アベイラビリティ，保守性，安全性）に関する国際規格（IEC 62278）をはじめ，列車制御システムに関わる国際規格（IEC 62279（ソフトウェア），IEC 62280（伝送），IEC 62425（システム安全）など）が発行され，システムのライフサイクルならびにシステムの安全目標を表わす安全性インテグリティレベル（SIL）を定めて，体系的な安全性解析を行い，適切に対策を施すことが一層重要になっている。

＊　信号・情報技術研究部　列車制御研究室

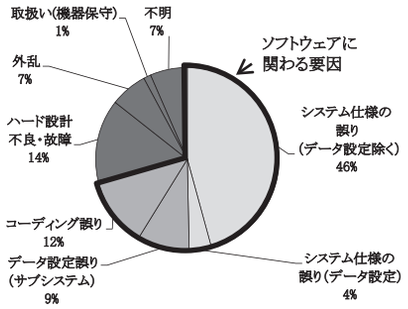

図１　電子連動端末部相当の開発段階での試験（5 カ月間）の障害分析結果

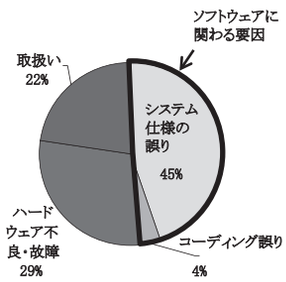

図２　電子連動装置論理部の運用段階（3 年間）の障害分析結果

2.2　障害原因

現状の列車制御システムにおける障害原因を把握するため，電子連動装置の障害データを分析した。電子連動装置は，論理部と端末部に大別される。論理部は端末部からの現場機器の状態情報を入力とし，各機器に対する出力を連動図表に従い決定する。端末部は論理部からの制御情報にもとづき信号機・転てつ機などを制御する。

図 1 に，ある事業者で開発，実用化された端末部に相当する装置の開発段階（現場設備との比較照合試験（5 カ月間））での障害分析結果を示す。また，ある事業者で運用されている電子連動装置の論理部の障害データ（導入開始してから 9 年経過後の 3 年間）を分析した結果を図 2 に示す。いずれの結果も，システム仕様に起因した障害が多く，仕様の作成段階においてシステム要件を明確にし，適切な対策を組み込むことが重要であることが分かる。

システム仕様の誤りの原因は，装置内の故障診断，処理性能等といったハードウェア仕様に依存したソフトウェア仕様，ならびに，入出力タイミングなど複数装置の接続構成に関わる仕様にあることが多く，これら仕様の明確化が重要である。

3．安全性確認手法

3.1　安全要件の課題と解決策

3.1.1　課題

これまで，安全性確認に用いる安全要件は，技術の進歩に合わせて整理が行われ，文書化が行われている[3) 4) 5)]。しかし，ライフサイクルの各段階で区別されておらず混在してまとめられており，また，装置単位での分類である。これでは，個々の安全要件は同一装置の後継機に対する適用に留まる。これら安全要件を活用するためには，(1) 機能単位での安全要件の定義と，(2) 安全要件の階層化管理が課題となる。

3.1.2　解決策

(1) 機能単位での安全要件の定義

安全要件は装置単位でなく，列車制御システムを構成する機能単位で作成する。また，ボトムアップ的な安全性技術の事例蓄積ではなく，各機能に必要となる安全要件を定義することとし，そのため，各機能内における個々の安全性技術の位置づけを明確化できる「安全要件のフォーマット」を定義する。

(2) 安全要件の階層化管理

多機能化した列車制御システムの構造が複雑化することを回避するためには，設計段階を概念設計と詳細設計とに区分した階層化設計が不可欠となる。よって，個々の安全性技術も同様に区分する。概念設計段階の安全要件は，装置横断的な共通の安全要件であり，同じ制御方式内では過去の安全要件を適用可能となる。また，個々の断片的な安全要件について，システム全体の中での位置づけが明確化されるので，技術継承の観点からも階層化は有効と考える。

以下，上記課題を解決すべく新たに提案する安全要件のフォーマット，ならびに，このフォーマットを活用したシステム仕様書の安全性確認手法について述べる。

3.2　提案する安全性確認手法

3.2.1　対象とする設計段階

概念設計段階における仕様の定義は，下位の詳細設計段階の仕様に大きく影響する。また，障害分析の結果からもシステム仕様に起因する障害件数が多いことが明らかになったので，対象は概念設計段階とする。この段階の安全要件は，「列車保安制御システムの安全性技術指針」と，個別の詳細設計を対象とする安全性技術との中間に位置し，従来まで不足していた安全要件を補完するものとなる。

3.2.2　安全要件のフォーマット

(1) 特徴と構成

新たに提案する安全要件のフォーマットの特徴は，システムに要求される安全要件を，対策の適用順を考慮し，「本質的な安全対策」と「追加の安全対策」に分類して体系的に構成した点である（図 3）。

安全要件は，列車制御システムを構成する機能単位で作成する。システムに内在する危険要因を根本的に排除するための制御論理やハードウェア構成といった本質的な安全対策は，基本仕様欄に記載する。また，追加の安全対策としての入力・処理・出力に対する故障診断，および異常検知後の制御は，安全性対策欄に記載する。

列車の間隔制御を例に述べると，本質的な安全対策としては，「各列車のルートが重ならない様に列車の間隔

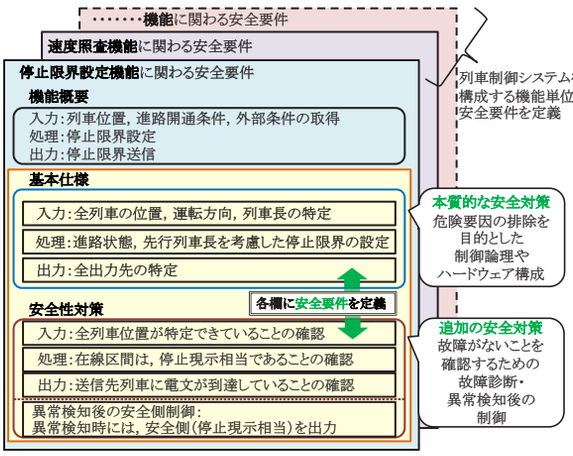

図３　提案する安全要件のフォーマット

制御を行うこと」が衝突防止のための制御論理に該当する。また，制御範囲内の 1 列車でも欠けた場合には制御論理が正しくても衝突するので，「全列車の位置を特定できていることの確認」という故障診断が追加の安全対策としてあげられる。

この定義は, ISO 12100（機械安全）における 3 ステップメソッド，つまり「本質的安全設計」,「安全防護及び付加保護」,「使用上の情報」の順での対策適用を参考に，対策の適用手順を考慮して定めた。この構造は，故障・誤り対策だけでなく，制御論理自体での安全確保の明確化を可能にする。また，列車制御システムにおいては，故障検知後の安全側制御と固定が重要であるので，「異常検知後の安全側制御」欄を定めた。

(2) 各欄の詳細

(a)「機能概要」欄

機能概要欄（図 3）の内容は，記載する基本仕様・安全性対策のもととなる情報であり，列車制御システムを構成する機能単位で記載する。機能には，FS-CPU ボード用の機能と列車制御アプリケーション機能とがある。この機能区分は，適用する対策目的の明確化に役立つとともに，ハードウェアの性能向上等に伴う設計変更がアプリケーション機能に与える影響範囲を最小限にする。このようにすれば, ハードウェア構成の種類に影響なく，アプリケーション機能を構築できる。

(b)「基本仕様・安全性対策」欄

図 3 に示す基本仕様・安全性対策欄は入力，処理，出力に分類して定義することで，対策の適用部位の差に起因する安全要件の漏れを極力排除することを図った。これら対策は, 安全性解析･評価において使用する FTA（故障木解析）の制約条件, FMEA（故障モードと影響解析）の検知手段とも関連づけて管理する。これにより，適用対策の目的の明確化，および，適用漏れの回避が期待できる。

3.2.3　安全性確認

安全要件のフォーマット（図 3）を用いて，作成されたシステム仕様書の安全性確認を行う（図 4）。

(1) ステップ 1：システム構成の定義と機能ブロック図の定義

列車制御システムに必要となる機能ブロックならびに機能間の入出力を定義するとともに，システム構成を定める。各機能の安全要件は図 3 に示すフォーマットを使用して作成する。

(2) ステップ 2：各機能の安全要件にもとづく確認

各機能の安全要件について，作成されたシステム仕様書を確認する。具体的には，列車制御システムの方式ごとに定めた安全要件の記載の有無を確認する。

(3) ステップ 3：列車制御アプリケーション機能ならびに FS-CPU ボード機能間の整合性確認

列車制御システムを構成する複数機能間での安全要件に関する仕様の整合性を確認する。具体的には，ステップ 2 で確認した仕様を対象に, 機能間の入出力関係, FS-CPU ボードに搭載するアプリケーション機能の対応付けなどをもとに，安全要件に関する仕様書記載内容の整合性を確認する。例えば，列車制御アプリケーション機能と FS-CPU ボード機能間の仕様の整合性, ならびに, 列車制御アプリケーション機能間の仕様の整合性について，作成されたシステム仕様書の確認を行う。

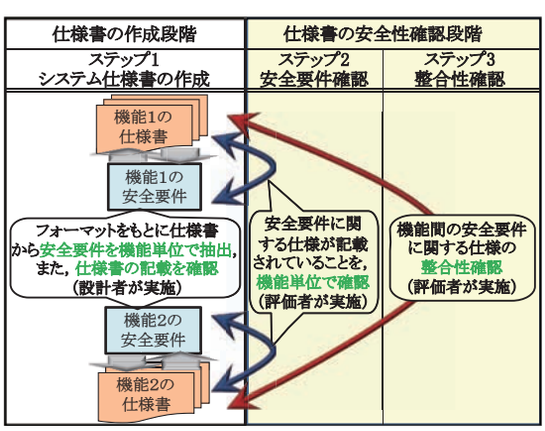

図４　提案するフォーマットを用いた安全性確認

４．安全性確認手法の適用例

提案する安全性確認手法の手順ならびに安全要件のフォーマットの確認のため，無線を用いた列車制御システム CARAT[6] の概念設計を一例に提案手法を適用する。CARAT は車上位置検知結果を地上装置に無線で伝送して先行列車との間隔制御や進路制御を行うシステムであり，近年 JIS 化された JRTC[7] とも本質的には機能が同じである。

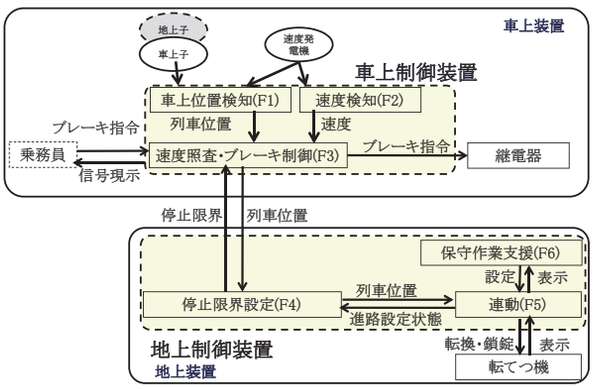

図５　CARAT を例とした列車制御アプリケーション機能ブロック

4.1　ステップ１：システム構成の定義と機能ブロック図の定義

CARAT を例とした列車制御アプリケーションの機能ブロックを図 5 に示す。また，FS-CPU ボードに関わる機能も含めた機能一覧を表 1 に示す。FS-CPU ボードに搭載する列車制御アプリケーション機能は，地上と車上でそれぞれ集約した構成とする（図 5）。以下，各機能の概要を述べる。

4.1.1　各機能の概要

(1) 列車制御アプリケーション機能

列車制御アプリケーション機能を表 1（F1 ～ F6）に示す。例えば，列車の間隔制御の要となる，地上制御装置内の「停止限界設定機能（F4)」を述べる。

(a) 列車位置，進路開通条件，外部条件の取得

全列車位置は，制御対象内の各車上制御装置から受信して取得する。また, 制御対象内の全進路の開通条件，外部条件を取得する。

(b) 停止限界の設定

制御対象内の全列車の停止限界は，進路の設定状況，全列車位置，外部条件にもとづき，設定する。

(c) 停止限界の送信

全列車の車上制御装置に対して停止限界を送信する。

(2) FS-CPU ボード機能

FS-CPU ボードの機能を表 1（F7 ～ F19）に示す。例えば，処理部（F8）の機能概要は，「入力値ならびに内部で保持する値をもとに，予め定めた内部演算を行い，出力値を算出する」となる。

4.1.2　安全要件の作成

安全要件は，基本仕様（制御論理もしくはハードウェア構成）と安全性対策に分けて，機能ごとに入力，処理，出力に分類して定める。

表１　列車制御システムを構成する機能の一覧

ID	分類		機能名称
F1	列車制御アプリケーション	間隔制御・進路制御	車上位置検知
F2			速度検知
F3			速度照査・ブレーキ制御
F4			停止限界設定
F5			連動
F6		保守作業支援	
F7	FS-CPU ボード	入出力・処理・照合	入力部
F8			処理部
F9			出力部
F10			照合部
F11		システム管理	冗長系管理
F12			モード（通常/保守）管理
F13			立ち上げ処理
F14			立ち下げ処理
F15			再立ち上げ処理
F16		保守	プログラム／データのダウンロード
F17			バージョン切替
F18			試験支援
F19			動作履歴・障害の管理

(1) 列車制御アプリケーション機能

「停止限界設定機能（F4)」内の処理における基本仕様ならびに安全性対策による安全性確保の例を表 2 に示す。この例では，安全性対策として示す安全要件は基本仕様と一部重なるが，何らかの故障・不良に伴う影響を考慮して，念のため診断を別途実施し，誤りがないことを確認することを目的とする点で異なる。なお，表 2 の安全性対策欄に示す故障診断で異常を検知した時には安全側制御（停止現示出力相当）を実施する。

列車制御アプリケーション機能の安全性対策欄に示す合理性チェックは，念のための診断としての位置づけであり，誤りを検出できない場合があることから，制御論理自体の信頼性が安全性確保において最も重要である。

(2) FS-CPU ボード機能

FS-CPU ボード機能（処理部（F8））における基本仕様と安全性対策による安全性確保の例を表 2 に示す。なお，表 2 の安全性対策欄に示す故障診断で異常を検知し

表２　安全要件の例

	基本仕様	安全性対策
F4 停止限度設定（処理） ※アプリケーション機能	・先行列車は，進路に応じて特定できること ・続行列車に対する停止限度の設定は，先行列車の列車長を考慮して，重ならないようにすること ・緊急停止情報と停止限界との関連性を明確化すること	・列車位置から停止限界までの区間が他列車と重なっていないことの確認
F8 FS-CPU ボード（処理部） ※ FS-CPU ボード機能	・A, B 系の独立性の確保 ・使用する割込み信号の特定と限定 ・処理負荷の管理 ・ノイズ等の外乱対策 ・キャッシュの更新 ・立ち上げ，立ち下げ処理と時間の特定 ・情報の安全側と危険側の区分（0,1 の定義） ・安全性が要求される箇所の分離，プログラム構造の単純化	・プロセッサにおける処理誤りの検出 ・クロックチェック ・電源電圧の低下チェック ・インループ状態になった場合の安全側固定 ・メモリ（ROM,RAM）チェック ・ECC 誤訂正対策 ・DPRAM チェック ・割り込み回路に対する診断 ・冗長系間の同期チェック ・処理順序のチェック

た時には，安全側制御（処理停止，出力停止）し，また，異常系の出力は確実に切り離す。

FS-CPU ボード機能では，ハードウェア故障検知と安全側固定が中心となるが，制御論理自体での安全性確保も重要であることがわかる。

4.2 ステップ 2：各機能の安全要件にもとづく確認

ステップ 1 で定めた各機能の安全要件が，作成したシステム仕様書に記載されていることを確認する。

4.3 ステップ 3：列車制御アプリケーション機能ならびに FS-CPU ボード機能間の整合性確認

(1) 列車制御アプリケーション機能間の整合性

列車制御アプリケーション機能間の整合性確認を，システム仕様書に対して行う。機能間の関係はステップ 1 で作成する機能ブロック図（図 5）にもとづき判断する。

例えば，「速度照査・ブレーキ制御機能（F3)」と「停止限界設定機能（F4)」間の入出力の整合性の確認項目の例としては，F4 からの出力である「停止限界」があげられ，機能間での停止限界の定義，合理性チェックの範囲などの整合性を確認する。

(2) 列車制御アプリケーション機能と FS-CPU ボード機能間の整合性

列車制御アプリケーション機能と FS-CPU ボード機能との整合性確認を，システム仕様書に対して行う。機能間の関係は，ステップ 1 で定めた，FS-CPU ボードに搭載するアプリケーション機能との対応づけをもとに抽出する。

例えば，各機能の処理部について述べると，FS-CPU ボードにおいて定めている「情報の安全側と危険側の明確な区分（0,1 の定義)」について，FS-CPU ボードに搭載されている列車制御アプリケーションの各機能は整合性がとれていることを確認する。

4.4 システム仕様書に対する確認項目数の検討

安全要件として図 3 の各欄に定めた項目に対して，新しく作成されたシステム仕様書と対比する。表 1 に示す機能をすべて実装した場合において想定される確認項目数は，ステップ 2 では，7 欄（図 3）× 19 機能＝ 133 欄，ステップ 3 では，7 欄（図 3）× 6 機能（列車制御アプリケーション機能）＝ 42 欄に対しての FS-CPU ボードに関わる 13 機能との比較となり，546 欄となる。また，通常機能における入出力の整合性の確認項目としては 5 機能間（図 5 内機能ブロック間インタフェース）× 7 欄 × 2（双方向）=70 欄となる。また，FS-CPU ボードに関わる 13 機能については，相互に影響しないことを確認するためには，$_{13}C_2$=78 の組み合わせに対する 7 欄の確認となり，546 欄となる。なお，各欄には確認項目の詳細が記載されるので，確認項目数は更に多くなる。

これらの結果から，安全要件を体系的に整理することが的確なシステム設計に有効であるほか，何らかの支援ツールの構築が必要と考える。

5．安全性確認支援ツールの構築

上述の提案する確認手法における確認項目数は多いことから，的確かつ効率的な実施を図るため，確認項目を自動生成する支援ツール（安全性確認支援ツール）を構築した。本ツールは，Microsoft Access で作成した。

5.1 ステップ 1：システム構成の定義と機能ブロック図の定義

列車制御システムの方式を定義し，各方式において必要となる機能を選択する。また，FS-CPU ボードを定義する。

対象装置のアプリケーション機能，ならびに，これら機能間の入出力関係を機能ブロック図に定義する。機能間の入出力関係は，機能ブロック図をもとに自動で判断することも可能であるが，列車制御システムの方式によって変わるものではないため，本ツールでは表 3 に示す関係を事前に既定値として組み込み，必要がある場合のみ変更する構成とした。例えば，表 3 の 1 行目は，車上位置検知（F1）機能が，速度照査･ブレーキ制御（F3）に対する出力を有することを示す。この機能間の入出力関係をもとに，機能間の整合性確認項目を自動生成する。

また，FS-CPU ボードに対する機能も定めるとともに，各 FS-CPU ボードに搭載するアプリケーション機能を定める。ステップ 3 では，これら機能間の関係をもとに，アプリケーション機能と FS-CPU ボードに関わる機能間の整合性確認項目を自動生成する。

表３　機能間の入出力定義

機能名（ID）	入力			出力	
	入力 1	入力 2	入力 3	出力 1	出力 2
車上位置検知（F1）				F3	
速度検知（F2）				F3	
速度照査・ブレーキ制御（F3）	F1	F2	F4	F4	
停止限界設定（F4）	F3	F5		F3	F5
連動機能（F5）	F4	F6		F4	F6
保守作業支援機能（F6）	F5			F5	

5.2 ステップ 2：各機能の安全要件にもとづく確認

機能ごとに定めた安全要件について，システム仕様書への記載を確認する。記載を確認できた時は，確認済みの印をつける。また，各安全要件には，設計仕様書に記

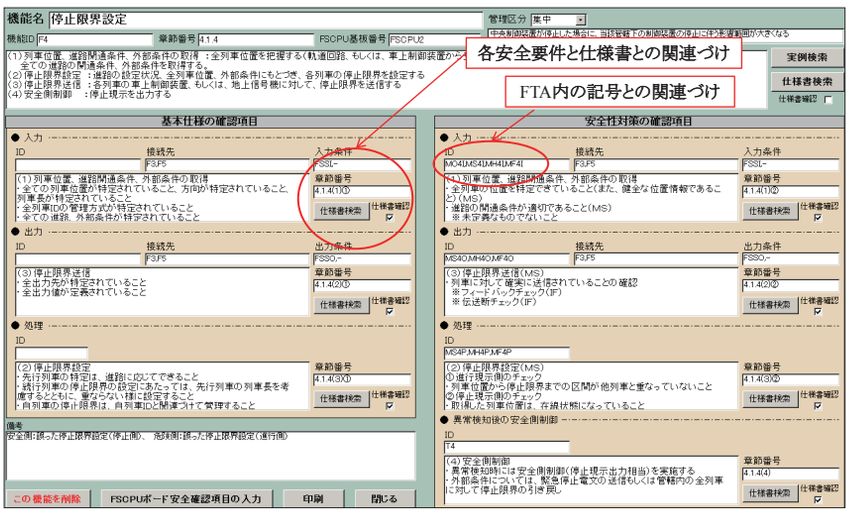

図６　安全要件にもとづく確認画面

載されている章節番号を関連づける。FTA の制約条件とも関連づけ，対策の位置づけを明確化する（図 6）。

5. 3　ステップ 3：列車制御アプリケーション機能ならびに FS-CPU ボード機能間の整合性確認

仕様書記載の安全要件に関わる内容の整合性は，ステップ 1 で定めた機能ブロック図に示す機能間の入出力関係等をもとに確認する。安全性確認支援ツールは，ステップ 2 で定めた，安全要件と設計仕様書との関連情報をもとに接続先の設計仕様書を表示し，整合性の確認支援を行う。

具体的には，アプリケーション機能の整合性の確認項目は，機能ブロック図に示す機能間の入出力関係（表 3）をもとに自動生成する。また，アプリケーション機能と FS-CPU ボードに関わる機能との整合性の確認項目は，ステップ 1 で定める FS-CPU ボードに搭載する機能の割り当て情報をもとに自動生成する。なお，FS-CPU ボードに関わる機能の整合性確認項目は，搭載するアプリケーション機能だけでなく，他の FS-CPU ボードに関わる機能相互に影響することを考慮して自動生成している。

6．おわりに

列車制御システムの安全性確保には，対策を適切に漏れなく適用することが重要である。それを的確に実施するため，システムを構成する機能に着目した安全要件のフォーマット，ならびにこのフォーマットを活用した安全性確認手法を提案した。また，無線を用いた列車制御システム CARAT を一例に，この提案手法を適用する手順を示した。この手法にもとづいて安全性確認を効率的に実施するため，システム設計仕様書の安全性確認項目を自動生成する安全性確認支援ツールを試作した。これら安全要件は，同様の制御方式であれば再利用可能である。また，技術継承にも役立つものと考える。

文　献

1）秋田，渡辺，中村 : 電子連動装置 SMILE の開発 , 鉄道技術研究報告 No.1361, 1987
2）遠藤，国藤 : 駅構内ネットワーク信号制御システムの開発 , JR East Technical Review No.20, 2007
3）信号における安全性技術調査書，信号保安協会，1978
4）マイクロエレクトロニクス信号保安装置の安全性検討会 : 信号保安装置へのマイクロエレクトロニクス導入指針，鉄道技術研究所速報，NO.A-83-147，1983
5）鉄道総研 : 列車保安制御システムの安全性技術指針 ,1996
6）岩田，西堀，平尾 : 無線による列車制御システム CARAT の事前安全性解析，鉄道総研報告，Vol.13, No.8, pp.39-44, 1999.8
7）無線式列車制御システム，JIS E 3801-1，2009