(鉄道総研月例発表会講演要旨)

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

信号・情報技術研究部　列車制御研究室
主任研究員　岩田 浩司

1. はじめに

列車制御システムは，信号機・転てつ機などの装置を制御し，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対策が施される。近年，列車制御システムは多機能化し，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対策が求められる。そのためには，システムを構成する機能ごとに安全要件を定めて体系的に管理し，システム全体を定義する仕様書（システム仕様書）に確実に反映する仕組みが必要である。そこで，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用いたシステム仕様書の確認手法を提案する。以下，無線を用いた列車制御システムを一例に提案手法，ならびに，提案手法の手順確認のために試作した確認支援ツールを紹介する。

2. 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)]，保安装置用処理ボード（以下，フェールセーフCPUボード：FS-CPUボード）とそのソフトウェアで実現される機能は，保守性の向上などにより多種類となっている。一方，鉄道のRAMS（信頼性，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が発行され，システムのライフサイクルや安全目標（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。これまでも技術の進歩に合わせて，安全要件の文書化[2)~4)]が行われているものの，装置単位が基本であり，列車制御システムを構成する機能単位で安全要件は定義されていない。また，列車保安制御システムの安全性技術指針[4)]に定める安全性確保のための基本原則の適用にあたっては経験を要するので，既に示されている安全要件を充実し，より使いやすい形にすることも重要である。

列車制御システムにおける障害原因を把握するため，開発段階における電子連動装置の障害データを分析した。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）での障害分析結果を示す。システム全体の仕様（システム仕様）に起因する障害は50%を占めており，設計当初に定める仕様書における安全要件などの記載洩れ低減，矛盾低減が必要である。

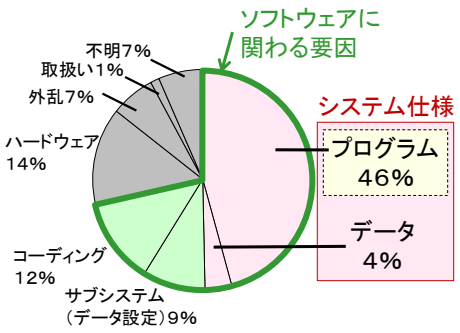


図1　電子連動端末部相当の開発段階での試験（5カ月間）の障害分析結果

このように，障害分析の結果からシステム仕様に起因する障害件数は多く，またライフサイクル上流の設計段階で定める仕様の誤りは後段の詳細設計・製造段階の仕様に大きく影響する可能性がある。これらを考慮し，検討対象は上流の設計段階（概念設計段階）で定義する，システム仕様書における安全要件とする。

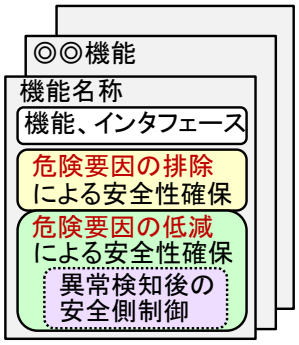


図 2 提案する安全要件のフォーマット

3. 提案する安全要件のフォーマット

提案する安全要件のフォーマットの特徴は，安全対策の目的・手段の相違を明確にするため，「危険要因の排除」と，これが難しい場合の「危険要因の低減」に分けて予め欄を設けた点である（図 2）。「危険要因の排除」欄には，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における本質的な安全対策を記載する。また，この危険要因の排除が難しい場合には，故障診断を適用して危険要因の低減をはかるが，この対策は「危険要因の低減」欄に記載する。このフォーマットの利点は，予め欄を設けた構成とすることにより，比較的安全対策を記載しやすい故障や誤り検知のための診断だけでなく，制御論理・ハードウェア構成における危険要因の排除のための考慮事項も明確にできる点である。また，診断で異常検知後の安全側制御と安全側固定についての仕様書への定義漏れ防止も期待できる。

処理装置における危険要因の排除の例としては，比較対象となる二つの系間での共通原因故障を排除するための独立性の確保があげられる。また，危険要因の低減策の例としては，メモリチェックなどの故障診断があげられる。この故障診断で異常を検知した時には，安全側制御（処理停止）させる。

このような安全要件のフォーマットに従って，列車制御システムを構成する機能単位の安全要件を作成する。

4. 提案する安全性確認手法

機能単位の安全要件は，提案する安全要件のフォーマットをもとに確認可能であるが，複数機能で構成されるシステム全体における安全要件に関わる仕様の整合性の確認は必要となる。そこで，これら確認の手順を体系的に定め，システム仕様書に対する安全性確認手法として提案する（図 3）。

以下，各ステップについて述べる。

(1)ステップ 1：システム仕様書・安全要件の作成

仕様書の作成段階では，列車制御システムの機能ブロックならびに機能

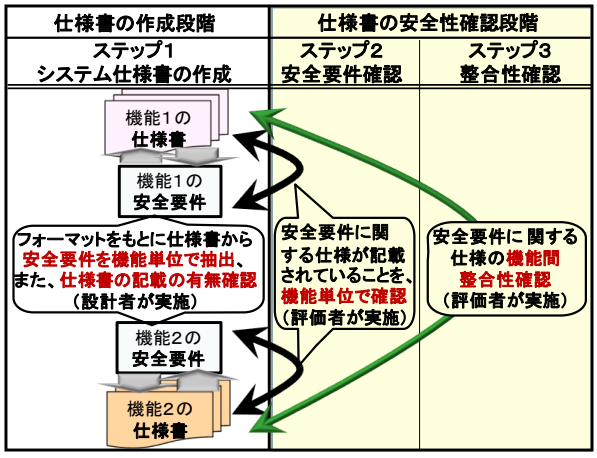


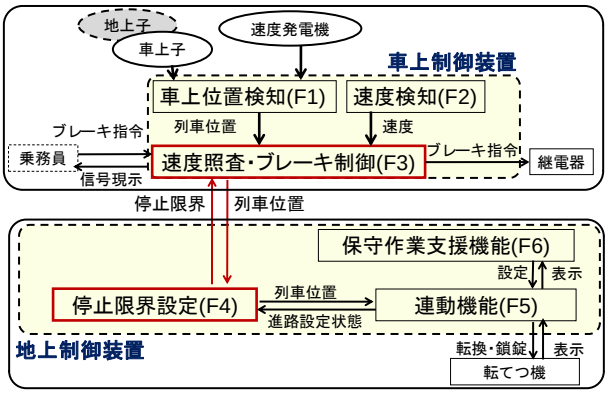
図 3 提案する安全要件のフォーマットを用いた安全性確認手法

間の入出力を定義し,システム構成を定める。また,各機能を定義するとともに,各機能の安全要件を図 2 に示すフォーマットを使用して作成する。

(2)ステップ２：安全要件にもとづく確認

作成したシステム仕様書に対して,ステップ１で定めた列車制御システムを構成する各機能の安全要件をもとに,仕様書への記載の有無を確認する。この確認作業は,設計者と異なる評価者が実施する。

(3)ステップ３：列車制御システムを構成する機能間の整合性確認



※()は機能IDを示す

図 4 CARAT を例とした列車制御アプリケーション機能ブロック

列車制御システムを構成する機能間での安全要件に関する仕様の整合性を確認する。この確認作業は，ステップ２と同様に設計者と異なる評価者が実施する。

機能間の整合性確認が必要となる箇所は,機能間の入出力に関わる箇所,ならびに,FS-CPUボードに搭載するアプリケーション機能の割り当てに伴う箇所があげられる。これらについて，安全要件に関する仕様書記載内容の整合性を確認する。

具体的には，機能間の整合性確認は，機能ブロック図にもとづき判断する。列車制御アプリケーション機能の例として，図 4 に車上位置検知結果を地上装置に無線で伝送して間隔制御を行う，CARAT[5]の機能ブロック図を示す。CARAT は，近年 JIS 化された JRTC[6]とも本質的には機能が同じである。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一つとして,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内容,また,これら定義にもとづく合理性チェックの範囲などの整合性を確認する。

また，列車制御アプリケーション機能と FS-CPU ボード機能との安全要件に関わる仕様の整合性確認は，FS-CPU ボードに割り当てるアプリケーション機能との関係をもとに行う。例えば，FS-CPU ボードにおける「情報の安全側と危険側の明確な区分（0,1 の定義）」が，列車制御アプリケーションの各機能における考え方と合致していることを確認する。

5. 提案手法のケーススタディ

提案する確認手法は，仕様書の確認手順を体系的に定めており，確認項目を特定でき,確認の進捗状況も把握できる。その一方,確認項目数が膨大となる可能性があり,的確かつ効率的な実施を図る必要があると考え，確認支援ツールを作成した。ここでは，アプリケーション機能として無線を用いた列車制御システム CARAT と FS-CPU ボードを一例に，確認項目の提示と確認結果を管理するツールを試作した。本ツールは，Microsoft Access で作成した（図 5)。

この確認支援ツールを用いて，提案手法の手順が実際に行えることを確認した。まず，列車制御アプリケーション機能（6 機能）と FS-CPU ボードの各機能（13 機能）

の安全要件を機能単位に分割して定め，それぞれの安全要件を設計者の視点で入力した（ステップ１）。また，ツールでは，機能単位の仕様と安全要件との関係を章節番号でトレース可能とし，この情報を用いて安全要件が仕様に反映されていることを評価者の視点で確認し，確認結果欄に印をつける構成とした（ステップ２）。さらに，機能間の不整合がないことの確認は，入出力関係のある機能を抽出して評価者に提示して確認する構成とした（ステップ３）。今回のケーススタディの規模での確認項目数は，ステップ２では機能数 19 と，安全要件の項目欄（危険要因の排除（3 欄）と危険要因の低減（4 欄））を積算した 133 欄となった。さらに，ステップ３の整合性確認では機能間の入出力の組み合わせが確認項目に加わることから，提案手法は実施可能であるものの，効率的な実施には機械的に確認項目を提示し，確認結果を管理する支援システムの併用が効果的であることを確認した。

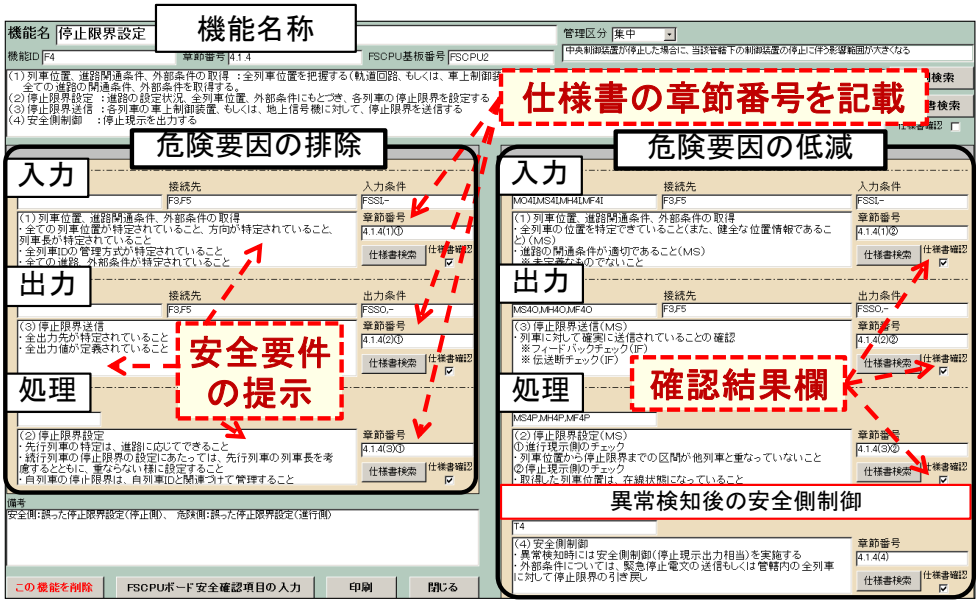


図 5 安全要件にもとづく仕様書の確認画面の例

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。これら作業を的確に実施するため，機能単位での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。無線を用いた列車制御システム CARAT を一例に，この提案手法の適用手順を示した。作成した安全要件は，技術継承にも役立つものと考える。今後，提案手法を適用するにあたっての技術的なアドバイスなどを実施していきたい。

参考文献

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)信号における安全性技術調査書，信号保安協会，1978

3)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

4)鉄道総研: 列車保安制御システムの安全性技術指針，1996

5)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，1999.8

6)無線式列車制御システム，JIS E 3801，2009