列車制御システムの安全性を仕様段階で確認する

近年，列車制御システムはネットワーク化され，保守性向上などのため多機能化しています。このシステムには高いレベルの安全性が要求され，ソフトウェアだけでなくハードウェア，また機器単体に加えて列車制御システム全体としての安全性対策が必要です。よって，システムを構成する機能単位での安全要件を定めて体系的に管理し，これらを確実に組み込む仕組みが必要と考えます。そこで，機能単位での安全要件のフォーマット，ならびに，この安全要件のフォーマットを活用した安全性確認手法を提案するとともに，この確認作業を的確に実施するための支援ツールを作成しましたので紹介します。

岩田　浩司
Koji Iwata
信号・情報技術研究部
列車制御研究室
主任研究員
［専門分野］列車制御システム，安全性

列車制御システムの状況

列車制御システムは，列車間の衝突や脱線を防止するための信号機・転てつ機を制御する高い安全性が要求される装置です。新幹線のATC（Automatic Train Control：自動列車制御装置）では，地上制御装置と車上制御装置間の信号伝送にレールを用いています。近年は，地上と車上間の伝送に無線を用いたシステムも実用化され，システムを構成する機器数は多く，相互に多くの情報を伝送し，システムは複雑化しています。

列車制御システムの安全性

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[1]しています。万一，列車制御システムが故障して停止信号を進行信号と誤った場合，重大な事故に至る可能性があります。このため，故障時の安全対策を施した保安装置用処理ボード（以下，FS-CPUボード）が用いられています。FS-CPUボードでは，例えば処理中の誤りを検出するため，同一処理を2つのCPUで行い，相互に照合しています。誤りがある場合には停止信号とな

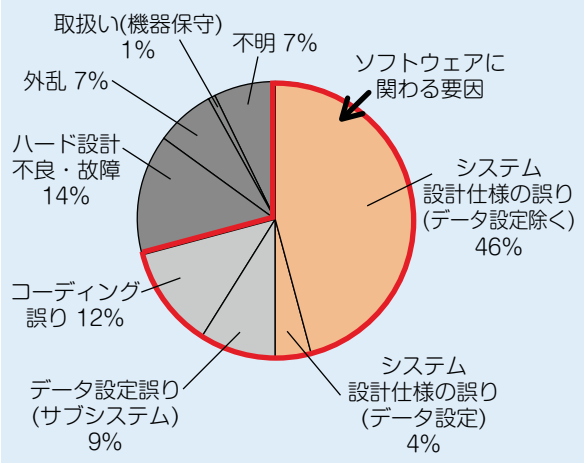

図1　開発段階での試験（5カ月間）の障害分析結果
（電子連動装置を構成する一装置を対象）

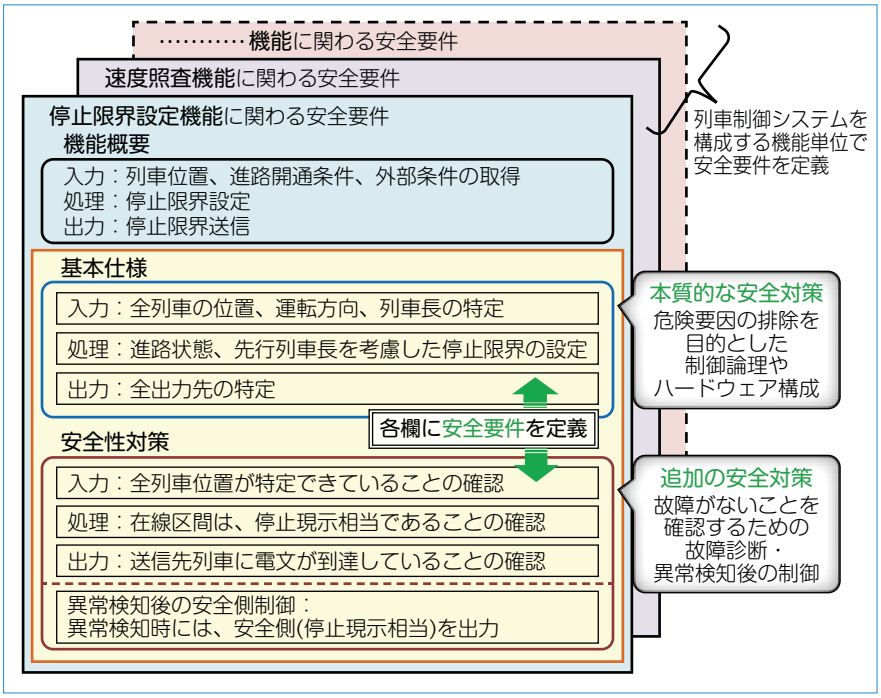

図2　提案する安全要件のフォーマット例

るフェールセーフなハードウェア構成としています。この処理ボードに搭載されるソフトウェアで実現される機能は，CPU処理性能の向上とともに保守性向上などのため，多種類となり論理は複雑化しています。

新しいシステムの構築時には，その安全性を確認するため，設計段階からFTA（Fault Tree Analysis：故障木解析），FMEA（Failure Mode and Effects Analysis：故障モードとその影響解析）などの安全性解析が行われます。これらの解析結果も用いて動作確認試験は行われます。これらの取り組みにより，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ます。

近年は鉄道のRAMS（信頼性，可用性：アベイラビリティ，保全性，安全性）規格IEC 62278など，列車制御システムの国際規格が発行され，RAMSを観点としたシステムの立証のための文書化が求められつつあります。

システム設計仕様書と安全要件

列車制御システムは，多くのサブシステムで構成されます。個々の構成要素であるサブシステムの仕様が正しくても，システム全体としては不安全になる可能性があります。よって，サブシステムの詳細設計仕様の決定には，システム全体としての動作を定義するシステム設計仕様書が必要です。この動作を定める文書がシステム設計仕様書です。

システム設計仕様書は，試験段階での確認項目の設定にも必要です。障害分析の結果（**図1**）からもシステム設計仕様に起因する障害件数が大きな割合を占めており，設計初期の段階で作成するシステム設計仕様書で明確に定義し，適切な対策を組み込むことが重要です。そこで，システムを構成する機能単位で定めた安全要件を体系的に作成し，システム設計仕様書に対する確認項目として，提示することとしました。

安全要件は，これまでも技術の進歩に合わせて整理が行われ，文書化も行われています[2)~4)]。基本的な安全性確保の基本方針は，鉄道総研が事務局となり作成した「列車保安制御システムの安全性技術指針」に定められています。今回新たに定める安全要件は，この基本方針と，個別の詳細設計例とを体系的に結びつけるためのものです。この安全要件はシステムを構成する機器が多く，複雑化してきていることからも必要なものです。

提案する安全要件のフォーマット

新たに安全要件を定義するための，フォーマットを定めました。この特徴は，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す（**図2**）。

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します。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，基本仕様欄に記載します。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します。

この安全対策の適用順は，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定めました。

この構造は，故障・誤り対策だけでなく，一見ではわかりにくい制御論理やハードウェア構成による安全確保の明確化を目的としたものです。また，列車制御システムにおいては，故障検知後に出力を安全側に制御するとともに，再度入力があってもその安全な状態を保持しておくことが重要であるので，「異常検知後の安全側制御」欄を定めました。

安全要件を用いた安全性確認手法

次に，この安全要件のフォーマット（**図2**）を用いて，作成されたシステム設計仕様書の安全性確認を行います。以下，提案する安全性確認手法の手順（**図3**）について，無線を用いた列車制御システムCARAT（Computer and Radio Aided Train control system）[5]の概念設計を一例に紹介します。

CARATは車上位置検知結果を地上装置に無線で伝送して列車の間隔制御を行うシステムであり，近年JIS化されたJRTC（Japan radio train control system）[6]とも本質的には機能は同じです。

ステップ1：システム設計仕様書の作成

この段階では，機能ブロックならびにハードウェア構成を定義します。CARATの機能ブロックを**図4**に示します。安全要件は，先に述べたように基本仕様（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，機能ごとに定めます。

FS-CPUボードに関わる機能では，ハードウェア故障検知と故障検知後に安全側に固定することが中心となります。しかし，故障を検知するための比較対象となる別系との独立性などのハードウェア構成自体での安全性確保も重要です。

また，安全性対策に示す合理性チェックは，処理中の誤りを想定した念のための診断で，すべての誤りを検出することはできません。基本仕様による安全性確保として示した制御論理自体の信頼性が安全性確保に重要です。

このように，安全要件のフォーマットを用いて区分けすることで，それぞれの目的を明確にすることができます。

ステップ2：各機能の安全要件にもとづく確認

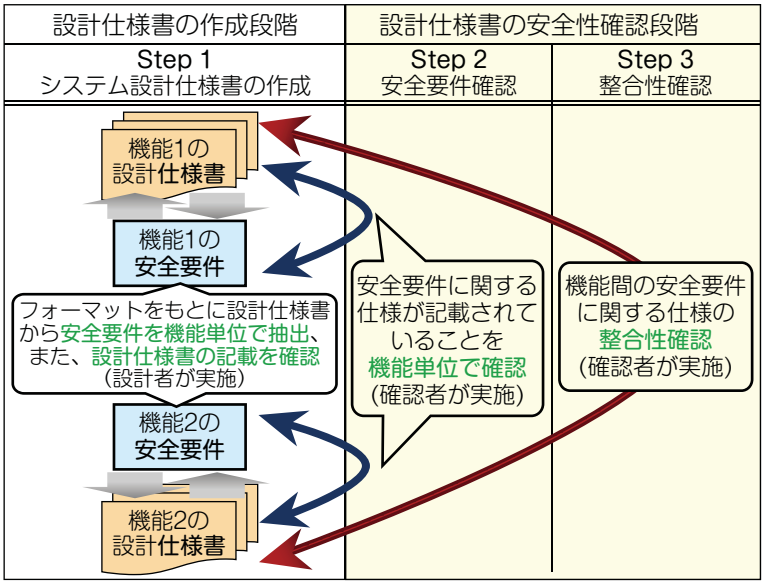

図3　安全要件を用いた安全性確認手法

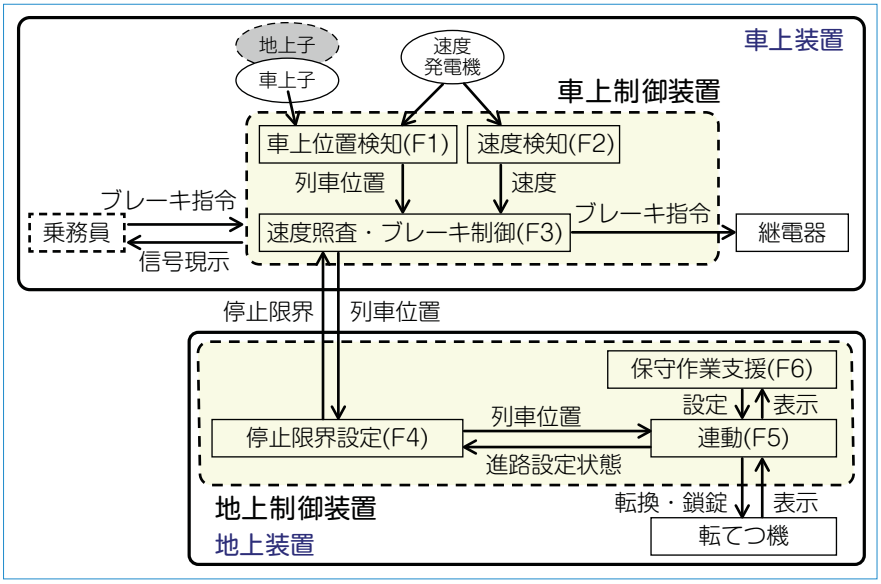

図4　CARATを例とした列車制御アプリケーション機能ブロック（通常機能）

ステップ1で定めた各機能の安全要件をもとに，設計者とは別の確認者がシステム設計仕様書を確認します。第3者が確認することで，設計者が気づきにくい誤りを見つけることができます。

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

この段階では，FS-CPUボード機能ならびに，これに搭載される列車制御アプリケーション機能間でのシステム設計仕様書の整合性確認を，安全要件のフォーマットに示す各欄について行います。

機能間の相互の関係はステップ1で作成する機能ブロック図（**図4**）にもとづき判断します。例えば，「速度照査・ブレーキ制御機能」と「停止限界設定機能」間の入出力の整合性の確認項目の例としては，停止限界設定機能からの出力である「停止限界」があげられ，機能間での停止限界の定義，合理

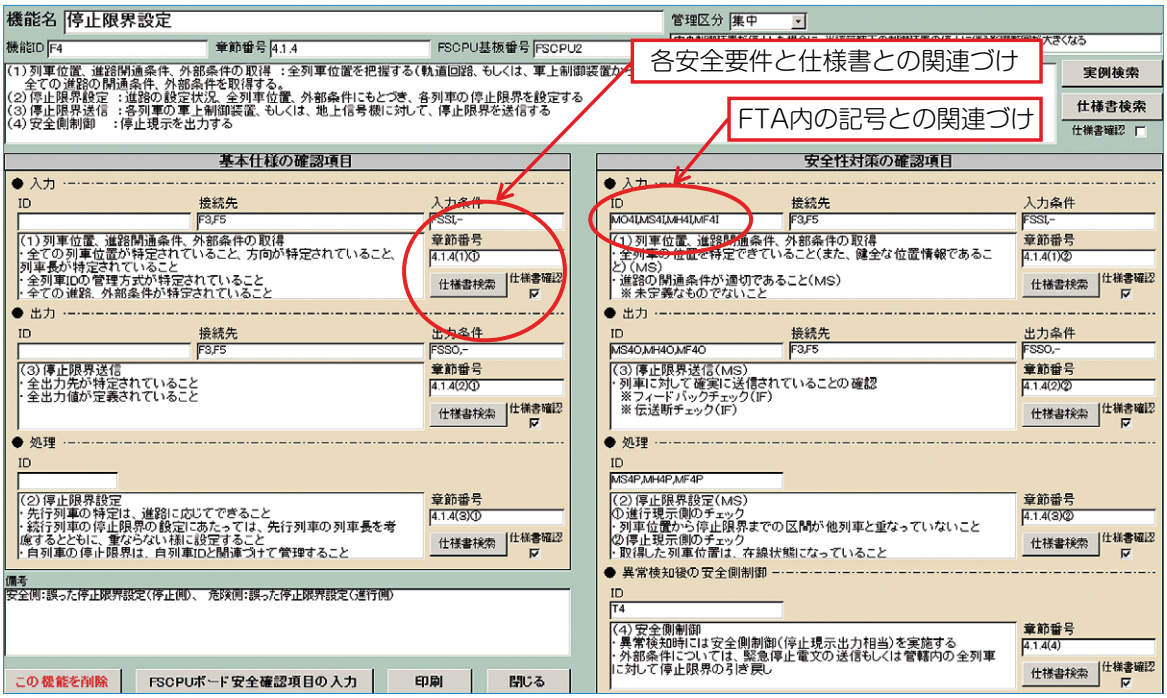

図5　安全性確認支援ツールによる安全要件の提示例

性チェックの範囲などについて，仕様書に定めた内容の整合性を確認します。また，列車制御アプリケーション機能とFS-CPUボード機能との整合性については，例えばFS-CPUボードにおいて定める「情報の安全側と危険側の明確な区分（例えば0を安全側，1を制御出力とした値の定義）」が，列車制御アプリケーションの各機能の定義と矛盾していないことを確認します。

安全性確認支援ツールの構築

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，確認項目を自動提示する支援ツール（安全性確認支援ツール）を構築しました。本ツールは，Microsoft Accessで作成しました。

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は，機能ブロック図をもとに自動で判断することも考えましたが，列車制御システムの方式が定まれば変わるものではないので，本ツールでは機能ブロック図の入出力関係を表形式で事前に既定値として組み込み，必要に応じて変更する構成としました。

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提示します。

また，各安全要件について，システム設計仕様書への記載を確認します。記載を確認できた時は，確認済みの印をつけます。

各安全要件は，設計仕様書の章節番号や，FTAの制約条件とも関連づけ，対策の位置づけを明確化できるようにしています（**図5**）。

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す。これら作業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ました。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，ならびに，この手法を的確に実施するために試作した安全性確認支援ツールを紹介しました。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す。また，技術継承にも役立つものと考えます。RRR

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