# 鉄道信号システムの安全性・信頼性向上に向けて

岩田　浩司
信号通信技術研究部（列車制御研究室　主任研究員）
いわた　こうじ

## はじめに

鉄道信号システムの安全性・信頼性向上のため，障害の発生頻度と影響度の組み合わせで定義される「リスク」による鉄道信号システムの評価，ならびに，システム設計において安全確保のため適用すべき要件（安全確認項目）を明確にすることに取り組んでいます。

ここでは，提案するリスク評価手法，ならびに，鉄道信号システムの中でも近年重要性が増しているソフトウェア要求仕様の安全確認項目について紹介します。

## 鉄道信号システムの安全性

鉄道信号システムは，列車の間隔を制御するための信号機や，線路の振り分けを行う転てつ器などを制御しており，高いレベルの安全性が要求される装置です。

この安全レベルを確保するため，設計段階においては障害にいたる原因を特定するためのFTA（故障の木解析：Fault Tree Analysis），ならびに，機器の故障に伴う影響を特定するためのFMEA（故障モードとその影響解析：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ます。

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ボードのソフトウェアで実現された機能は，CPU処理能力の向上とともに多様化し，保守性などの向上が図られています。近年は，装置間のネットワーク化，機器の小型化も進み，現場機器である信号機自体も端末化したネットワーク信号システムも実用化されています[2]。

一方，RAMS（信頼性，アベイラビリティ，保全性，安全性）国際規格（IEC62278）のほか，鉄道信号を対象とした国際規格[3)～7)]が制定され，鉄道信号システムのライフサイクルと，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）を意識したシステム開発もなされつつあります。

## 鉄道信号システムのリスク評価

鉄道においては安全の確保が最優先です。その一方，近年は同時に高いレベルのアベイラビリティも要求され，故障による装置の停止時間が短いことが求められます。そこで，鉄道信号装置の安全性とアベイラビリティについて，単位時間あたりの障害発生頻度と障害に伴うコストの積として定義したリスクにより，相互の位置づけを解析する手法を検討しています。

鉄道信号装置のRAMS指標については，信頼性（R）と保全性（M）の向上がアベイラビリティ（A）と安全性（S）の向上につながるので，アベイラビリティと安全性が鉄道利用者に直接関わる指標となります。この両者を総合的に評価する指標としては，例えば，障害の発生頻度とその影響度の組み合わせで定義されるリスクが考えられます。このリスクの目標値を定め，リスクを目標値まで低減させるため，改善を図るべき鉄道信号装置を選定し，その装置にリスク低減策を適用します。この低減策は，アベイラビリティ改善と安全性改善の2種類に分けられます。実際に対策を適用する際には，低減策の適用による安全性とアベイラビリティへの影響，ならびに，対策に要するコストを算出し，費用対効果を確認します。なお，この対策検討は，安全性の目標値が社会的に受け入れられるレベルに達している領域を対象とします。

以上が基本的なリスク評価の考え方ですが，ここでは，まず現状のリスクを把握する手法と，改善対処すべきリスクが大きい装置を特定する手法について説明します。

ここでのリスクの算出では，ある鉄道信号装置の障害に伴うリスクを，鉄道信号装置の障害の発生頻度とその障害に伴うコスト（損失）の積と定義します。安全側障害$i$（列車は停止するものの死傷者を伴わない障害），危険側障害$j$（死傷者を伴う障害）の単位時間あたりの発生頻度を，それぞれ安全側障害の発生頻度$a_i$ならびに危険側障害の発生頻度$s_j$とします。また，安全側障害$i$，危険側障害$j$の発生

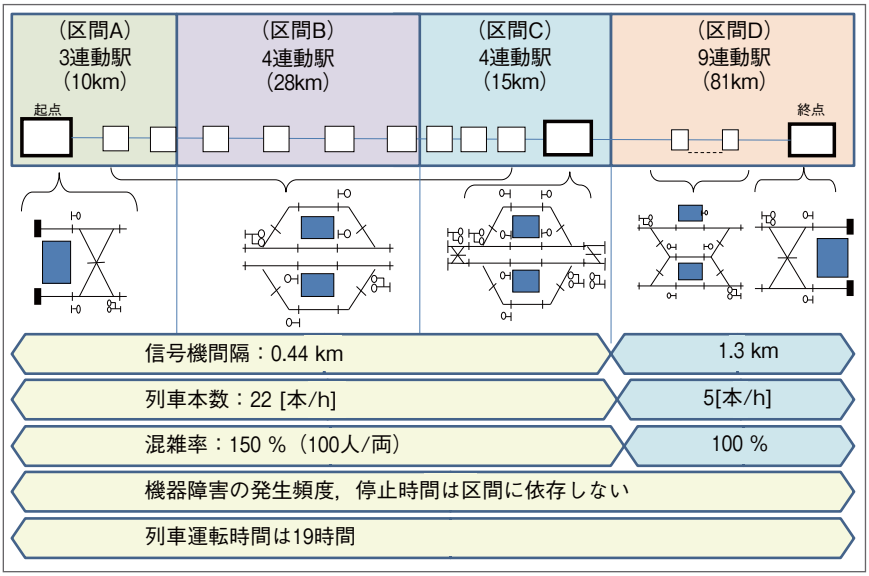



**図１　解析対象線区の構成**

による損失（人的損失，営業損失，物的損失の合計値）をそれぞれ安全側障害による損失$C_i$，危険側障害による損失$C_j$とすると，線区全体のリスク（$Risk$）は，その構成要素となる各装置のリスクの和として，以下のように表すことができます。

$$Risk = \Sigma\,(a_i \times C_i) + \Sigma\,(s_j \times C_j)$$

なお，個々の安全側障害$i$，危険側障害$j$は，FTA，FMEAにより抽出します。

## ケーススタディ

前述の評価法を，仮想的な解析対象線区を定めて適用しました。解析対象とした線区の構成を図１に示します。線区を区間Ａ～区間Ｄの４つの区間に分けました。折り返しは，線区の両端で行うと仮定しました。また，区間Ａ～区間Ｃと区間Ｄで運転本数が異なることから，区間Ｃ内の終点方の１駅においても折り返し可能としました。

解析対象とした鉄道信号装置は，図２に示す装置のうち，運行管理装置，転てつ機，連動装置，信号機，軌道回路です。また，各区間における装置台数を図３に示します。

障害発生頻度は，解析対象線区と類似した実線区の特定区間（約50km，15連動駅）の約５年分の障害データ（鉄道運転事故等届出書 第２号様式）を参考にしました。発生していない事象については，障害データを収集する対象範囲を拡大（約17,000km，約2,800連動駅）し，危険側障害は５年分，安全側障害は１年分の障害データから発生数を求め，装置数は特定区間との「距離比（327倍）」もしくは「連動駅数比（185倍）」で換算しました。当該エリアにおいても発生していない事象は，単位時間あたり$10^{-10}$と仮定しています。

機器の障害発生頻度，障害に伴う停止時間は区間に依存せず，列車運転時間は19時間と仮定しました。

コストについては，鉄道信号装置の障害による事故の影響度をETA（事象の木解析：Event Tree Analysis）により「大」，「中」，「小」，「なし」に分類し，それぞれのレベルに応じて，人的損失，営業損失，物的損失を仮定し，設定しました。

なお，本来は線区もしくは区間ごとにリスクの目標値を定めた上で改善対象装置を選定しますが，ここでは安全性とアベイラビリティの両面から改善対象装置を選定する手

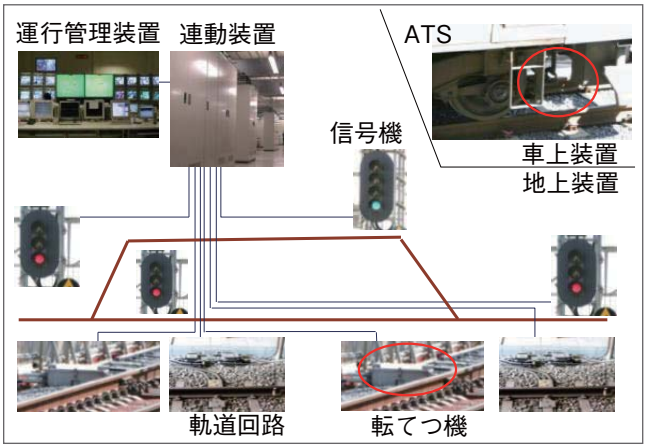



**図２　鉄道信号システムの装置構成**

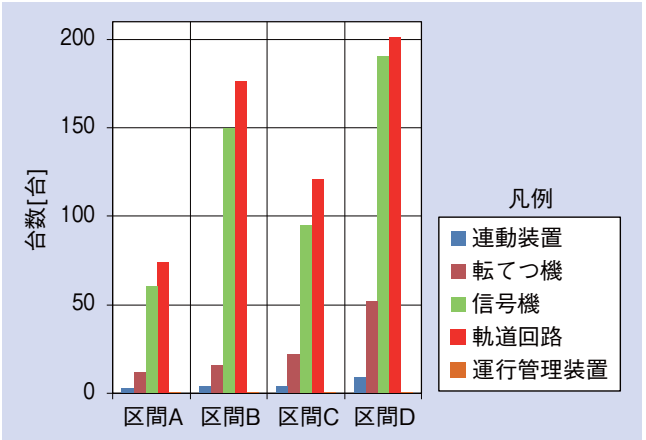



**図３ 解析対象線区における各区間の装置台数**

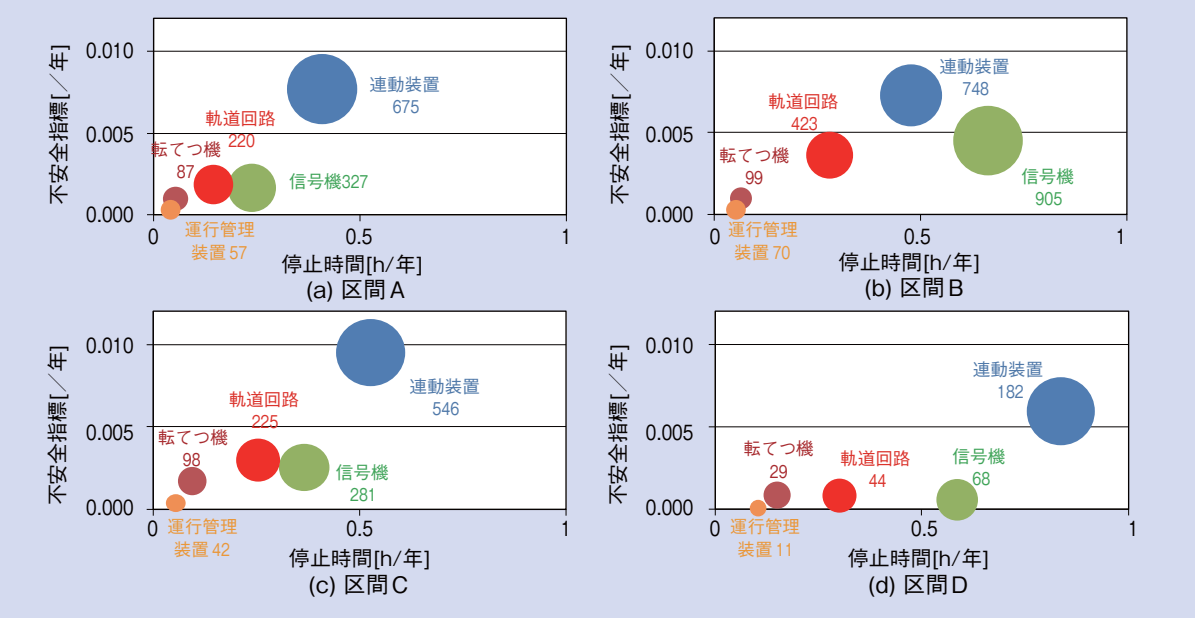



**図４　解析対象線区内における装置ごとの不安全指標，停止時間，リスク（暫定値にもとづく結果）**

法を紹介します。

図４に解析結果を示します。図４は，横軸にアベイラビリティに関わる「1年あたりの停止時間」を，縦軸に鉄道信号装置の障害発生時における事故の規模にもとづく1年あたりの死者数である「不安全指標」をとり，各装置のリスクを丸の大きさで示した図です。

基本的には，リスクの大きい装置は連動装置となり，不安全指標，停止時間ともに大きな値を示します。しかし，区間Bのように，リスクの大きい装置が信号機となる区間もあります。この理由としては，区間Bの駅中間の信号機数が多いことが一因としてあげられます。

前提として用いた数値は暫定値も用いていることから相対評価ですが，1年あたりの損失（リスク）にもとづく改善対象装置の選定における判断材料の一つとして役立つものと考えています。

不安全指標が十分低い値に抑えられている条件下での適用となりますが，リスクにより改善対象装置を特定する評価は，バランスのとれた積極的な投資の実現に役立つと考えています。

## 鉄道信号用ソフトウェア要求仕様の安全確認項目

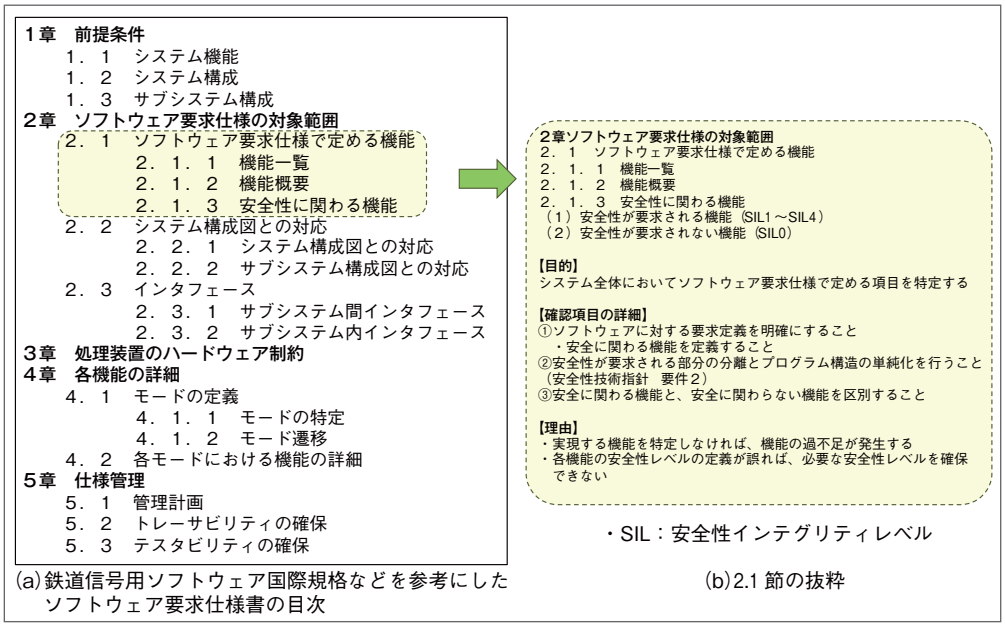
近年の鉄道信号システムは，多くの機能をソフトウェアで実現することができる様になってきています。この様な鉄道信号システムの構築においては，自由度の高い設計が可能となる利点があります。その一方，仕様書が明確に記述されている必要があります。

仕様書の作成にあたっては，システム全体としての設計仕様を定めた上で個別装置の仕様を定義すること，また，個別装置のソフトウェアを作成する際には，ハードウェア故障時の安全性対策が施されたフェールセーフCPUボードの特性を考慮した設計が必要です。

表１に，ソフトウェアに関わる品質向上策の例を示します。コーディングミス・設計仕様誤りなど，ソフトウェアを作成する段階での誤りは，検証ツールなどの適用（表１（a）），ならびに，共通化モジュールを定め，再利用を意識したアーキテクチャの構築（表１（b））により，低減されることが期待できます。しかし，ソフトウェアが実現すべき機能を規定する大元の仕様のうち，ソフトウェアで実装する箇所の最初の仕様書（ソフトウェア要求仕様）自体における仕様の漏れなどの誤りに対しては，十分ではありません。そこで，システム全体の仕様をもとに定める，鉄道信号システムのソフトウェア要求仕様の作成を対象とした安全確認項目を提案しています。

**表１　品質向上策の例**

| | |
|---|---|
| （a）開発支援ツール，検証ツールの活用 | ・鉄道用ソフトウェア（IEC62279）の規格を参考にしたドキュメント管理<br>・コーディングルールの適用（MISRA，など）<br>・フォーマルメソッドによる論理検証，検証済みのソースコードの自動生成によるコーディングミス防止，など |
| （b）再利用を意識したアーキテクチャの構築 | 誤り低減を目的とした再利用可能なアーキテクチャ定義<br>①共通化モジュールの特定（枯れたソフトウェア）<br>②共通化困難なモジュールの最小化（デバイスドライバ，など）<br>③仕様の共通化（競争領域）<br>④共通化しないモジュール（競争領域） |




(a)鉄道信号用ソフトウェア国際規格などを参考にしたソフトウェア要求仕様書の目次

(b)2.1 節の抜粋

**図５　鉄道信号用ソフトウェア要求仕様書における安全確認項目**

## ソフトウェア要求仕様の安全確認項目の概要

ソフトウェア要求仕様に対する確認項目は，鉄道信号用ソフトウェアの国際規格（IEC62279），列車保安制御システムの安全性技術指針[8]に示す項目，電子連動装置の機能仕様なども参考に設定しました。これら確認項目は，ソフトウェア要求仕様書の目次の形式で定めました（図5）。

以下，各章の目的を紹介します。

**(1)「1章　前提条件」**

システム全体の設計誤り，ハードウェアとソフトウェアの機能分担や物理的インタフェース等に起因するソフトウェア要求仕様の誤り防止を目的としています。

**(2)「2章　ソフトウェア要求仕様の対象範囲」**

機能の過不足防止のため，ソフトウェアで実現する機能を特定し，また，必要な安全レベルの確保のため，各機能の安全レベルを定義します。

**(3)「3章　処理装置のハードウェア制約」**

ハードウェアとソフトウェアの統合時の誤り防止のため，ハードウェアに関わる制約を特定します。

**(4)「4章　各機能の詳細」**

意図しない制御モードでの動作，誤出力の防止のため，全てのモードと遷移条件を特定します。

**(5)「5章　仕様管理」**

ソフトウェア品質の向上，仕様に関わる誤りの削減のため，仕様管理に関わる確認項目を定義します。

以上の確認項目は仕様管理，2号機以降の設計･製造管理，新規システムの仕様作成支援に役立つと考えています。

## おわりに

鉄道信号システムの安全性・信頼性向上のための取り組みとして，鉄道信号システムのリスク評価と，コンピュータ制御での鉄道信号システムの中で特に重要となるソフトウェア要求仕様の安全確認項目について紹介しました。

鉄道信号システムのリスク評価は，システムを構成する各装置の故障時の影響を明確化でき，投資効果の高い改善箇所の特定に役立つと考えています。今後，現段階で暫定値とした箇所のデータの充実をはかり，鉄道信号装置の効果的な改善に役立つように精度を高める所存です。

また，鉄道信号システムの安全確認項目は，特にソフトウェア要求仕様に着目して述べましたが，これは仕様管理，2号機以降の設計・製造管理，新規システムの仕様作成支援に役立つと考えています。

これらの取り組みにより，安心して利用できる鉄道信号システムの構築に貢献できればと考えています。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) 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) IEC62278：Railway applications - Specification and demonstration of reliability，availability，maintainability and safety（RAMS），2002
4) IEC62279：Railway applications - Communications，signalling and processing systems - Software for railway control and protection systems，2002
5) IEC62280-1：Railway applications - Communication，signalling and processing systems - Part 1：Safety related communication in closed transmission systems，2002
6) IEC62280-2：Railway applications - Communication，signalling and processing systems - Part 2：Safety related communication in open transmission systems，2002
7) IEC62425：Railway applications - Communication，signalling and processing systems - Safety related electronic systems for signalling，2007
8) 鉄道総研：列車保安制御システムの安全性技術指針,1996