（鉄道総研月例発表会講演要旨）

リスク評価と安全要件管理による列車制御システムのリスク低減

信号通信技術研究部　列車制御
主任研究員　岩田浩司

１．はじめに

近年の列車制御システムは高機能化した反面、ネットワーク化・ソフトウェア高依存となり、大規模かつ複雑化している。しかし、鉄道信号の機能に高いレベルの安全性が要求されることに変わりない。そこで、列車制御システムのリスク低減をはかるため、システムのリスク評価、及び、システムに適用すべき安全要件の管理の研究に取り組んでいる。本発表では、リスク評価手法とその適用結果を述べるとともに、鉄道信号システムの中でも特に重要なソフトウェア要求仕様の安全確認項目について述べる。

２．鉄道信号システムの安全性

列車制御（鉄道信号）システムは、信号機・転てつ機等、安全性が要求される装置を制御しており、高い安全性が要求される。この安全性レベルを確保するため、設計段階においては 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。

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、保守性等の向上が図られている。装置間ネットワーク化、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た[2)]。また、RAMS（信頼性、可用性、保守性、安全性）国際規格（IEC62278）など、鉄道信号に関わる国際規格[3,4,5,6,7)]が制定され、鉄道信号システムの開発ライフサイクルと、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る。

鉄道信号システムは、装置内のハードウェアとソフトウェアの安全性・信頼性だけでなく、これらを組み合わせた装置全体としての安全性、さらに、複数装置を接続した鉄道信号システム全体としての安全性が重要である。

以下、鉄道信号システム全体としての安全性・安定性に関わるリスクを低減するため、リスク評価、ならびに、ソフトウェア要求仕様の安全確認項目について述べる。

３．リスク評価

３．１　リスク評価の考え方

鉄道においては安全の確保が最優先であるが、近年同時に高いレベルのアベイラビリティも要求される。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提案し、モデル線区を対象としたケーススタディを試みた。

鉄道信号装置の RAMS 指標については、信頼性（R）と保守性（M）の向上がアベイラビリティ（A）と安全性（S）の向上に関係すると考えると、アベイラビリティと安全性が鉄道利用者

に直接関わる指標である。これら指標値は、鉄道信号装置が設置されている線区の重要性に基づき設定される。この重要性の評価指標としては、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る。この線区ごとのリスクの大きさにより、鉄道信号装置のアベイラビリティと安全性の目標値は定められる。

例えば、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）の積と定義する。安全側の障害 i（列車は停止するものの死傷者を伴わない障害）、危険側の障害 j（死傷者を伴う障害）の単位時間あたりの発生頻度は、それぞれ安全側障害発生頻度 a_i ならびに危険側障害発生頻度 s_j とする。また、安全側障害 i、危険側障害 j の発生による人的損失、営業損失、物的損失の合計値である安全側障害による被害額$_i$、危険側障害による被害額$_j$ とすると、リスク（*Risk*）はそれぞれの発生頻度と影響度を積算した式(1)で表すことができる。

$$Risk = \Sigma\ (a_i \times \text{被害額}_i) + \Sigma\ (s_j \times \text{被害額}_j) \qquad (1)$$

なお、個々の安全側障害 i、危険側障害 j は、FTA、FMEA により抽出する。

３．２　ケーススタディ

解析対象線区のモデルを表１に示す。区間は、区間 A～区間 D の４つに区分した。折り返しは、区間 A 内の起点と区間 D 内の終点でそれぞれ行う。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た（図１）。

解析対象装置は、運行管理装置、転てつ機、連動装置、信号機、軌道回路とした。各区間における装置台数を図２に示す。

障害発生頻度は、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）を基本とした。未発生事象については、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年分の障害データに基づき、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} と仮定した。

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、運転時間は 19 時間とした。

コストについては、鉄道信号装置としての障害による事故の影響度を ETA により「大」、「中」、

表１　解析対象線区

		区間 A	区間 B	区間 C	区間 D
区間長[km]		10	28	15	81
連動駅数	Type (a)	1	0	0	0
	Type (b)	2	4	3	0
	Type (c)	0	0	1	0
	Type (d)	0	0	0	8
	Type (e)	0	0	0	1
信号機間隔[km]		0.44	同左	同左	1.3
列車本数[本/h]		22	同左	同左	5
編成数[編成]		80	同左	同左	20
混雑率[%]（定員 100 人/両）		150	同左	同左	100

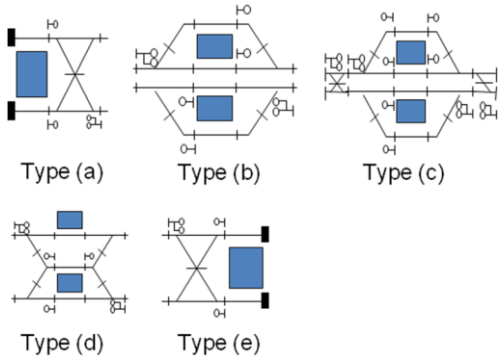

図１　連動駅の線形

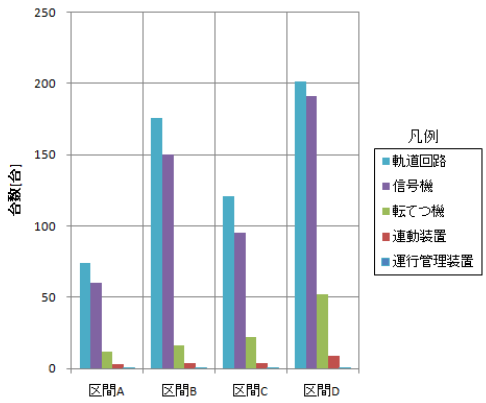

図２　モデル線における各区間の装置台数

「小」、「なし」に分類し、それぞれのレベルに応じて、人的損失、物的損失、営業損失の大きさを仮定して設定した。

以上の前提で、3.1 節に示す考え方に基づき算出した結果を図３に示す。設定値は暫定値も用いていることから相対評価となるが、１年あたりの損失の大きさ（リスク）に基づく改善対象装置の特定が可能であることが確認できた。不安全指標（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）が十分低い値に抑えられている条件下においては、リスクで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可能性がある。

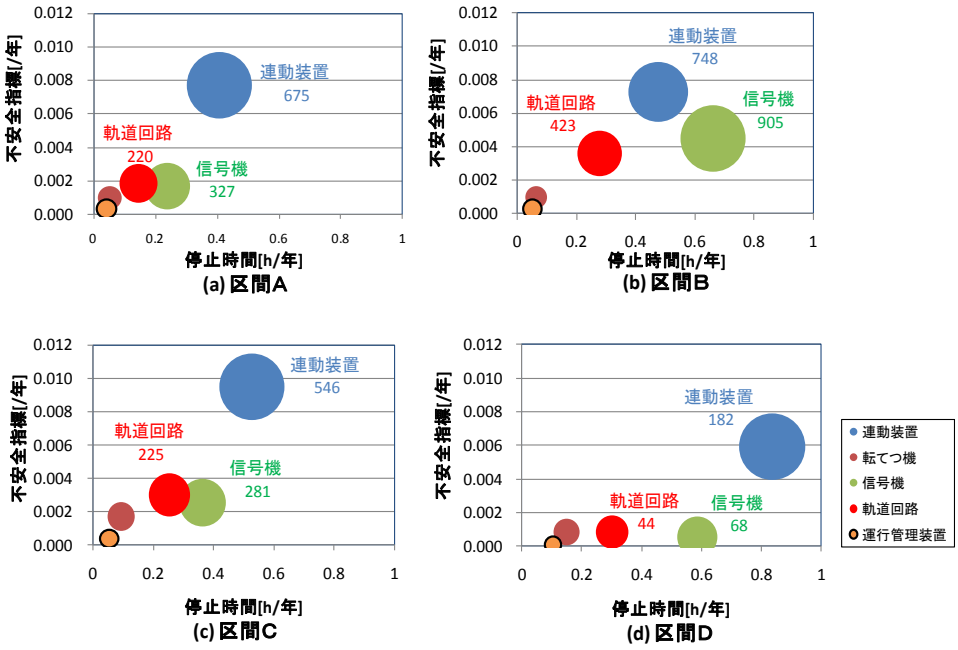

図３　モデル線区内における装置ごとの不安全指標、停止時間、リスク（暫定値にもとづく結果）
※円の大きさは１年あたりの損失の重み（リスク）

４．ソフトウェア要求仕様の安全確認項目

４．１　目的

近年の鉄道信号システムは、ソフトウェアで実現される機能が多い。この様な鉄道信号システムの構築においては、システム設計仕様が重要になる。また、基本的にはフェールセーフ CPU ボードの特性に基づきソフトウェアを作成するので、ソフトウェアに関わる仕様が特に重要になる。ソフトウェアに関わる誤り対策を表２に示す。コーディングミス・設計仕様誤りは、検証ツール等の適用（表２(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２(b)）により、低減することが期待できる。しかし、いずれもソフトウェアライフサイクルの最上流に位置づけられるソフトウェア要求仕様自体の漏れなどの誤りに対する課題は残る。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安全確認項目を提案する。

表２　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 ・コーディングルールの適用（MISRA、等） ・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、等
(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 ①共通化モジュールの特定(枯れたソフトウェア) ②共通化困難なモジュールの最小化(デバイスドライバ、等) ③仕様の共通化(競争領域) ④共通化しないモジュール(競争領域)

４．２　提案する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、国際規格（IEC62279（ソフトウェア））、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た（図４）。以下、各章の目的を示す。

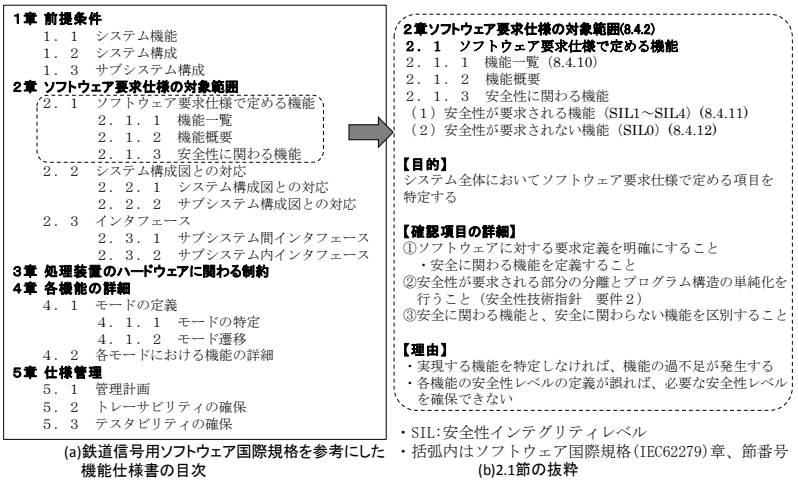

図４　鉄道信号用ソフトウェア要求仕様書における確認項目

（１）１章　前提条件

システム全体の設計誤り、ハードウェア・ソフトウェアの境界誤りによるソフトウェア機能仕様の誤り防止。

（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。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。

（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。

（４）４章　各機能の詳細

意図しないモードでの動作、誤出力の防止のため、全てのモードと遷移条件を特定。

（５）５章　仕様管理に関する確認項目

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、仕様管理を定義。

これら確認項目は、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る。

５．まとめ

鉄道信号システムの安全性・安定性に関わるリスク低減のため、リスク評価法ならびに安全要件管理について述べた。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る。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たいと考える。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る。今後、これら確認項目をより使い易くする手法を検討する。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る。

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)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