（鉄道総研月例発表会講演要旨）

# 電子連動装置のリスク評価

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

鉄道信号装置は、信頼性とともに高い安全性が要求され、設計段階から FTA（Fault Tree Analysis）、FMEA（Failure Mode and Effects Analysis）などの安全性解析によりフェールセーフを基本とした安全性対策が施される。この様な装置に対して、いかに効率的に安全性技術を組み込むかということは重要な課題である。また、鉄道信号装置の安全性に関する国際規格 RAMS (信頼性、アベイラビリティ、保守性、安全性) 規格 [1]などが制定され、今後システムの安全性をリスクの観点から解析・評価することが求められる可能性がある。よって、頻度と影響度というリスクの観点からこれまでの鉄道信号装置の安全性技術を再評価する方法について、電子連動装置を例として取り上げ紹介する。

## ２．対象装置

検討対象とする鉄道信号装置は最も高い安全性レベルが要求されるある事業者の電子連動装置である。電子連動装置は、論理部と端末部で構成される。論理部は端末部を介して現場機器の状態情報を入力し、連動図表に従い連動制御処理を行い、端末部に対して現場機器の制御情報を送信する。端末部は論理部から受信した制御情報にもとづき信号機・転てつ機を制御する。

論理部と端末部の導入台数（駅数）を図１に示す。論理部は導入開始後９年経過した機器、端末部はほぼ導入開始直後の機器を選定した。解析期間はいずれの装置も３年間である（図１）。障害解析は運行管理システムの障害管理表をもとに実施した。

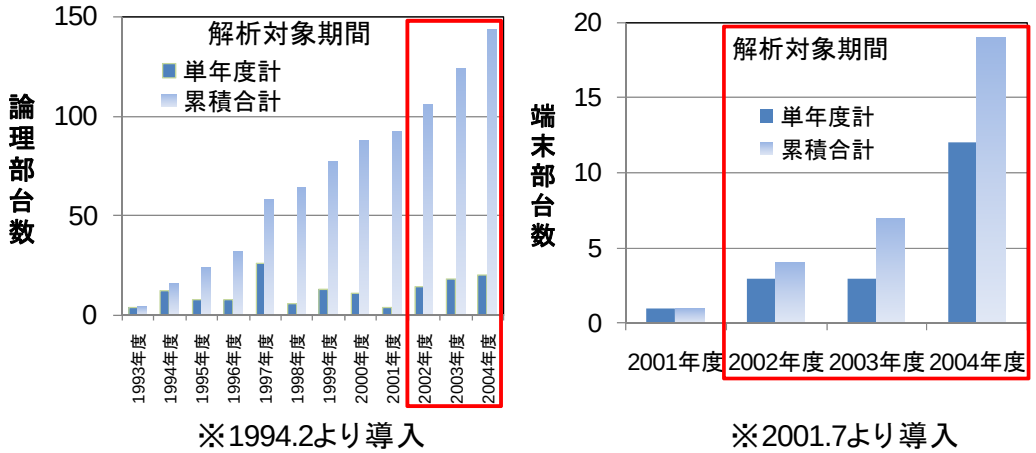


図１　論理部と端末部の導入台数の推移

## ３．ソフトウェア及びハードウェアの故障データ収集・分析

論理部、端末部に関する故障を分類した結果、論理部はシステム全体の仕様に関する原因、端末部はハードウェア（制御ボード）故障に関わる原因の占める割合が大きい（図２、図３）。

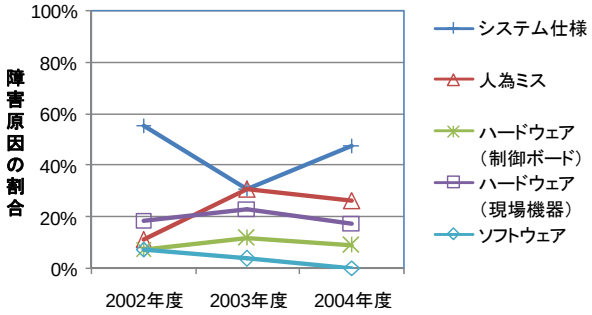


図２　論理部の障害原因の割合

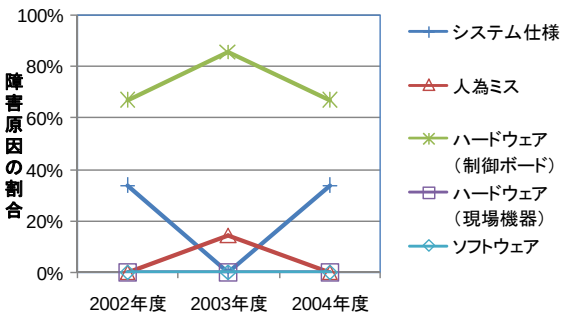


図３　端末部の障害原因の割合

この装置間での差の理由の一つとしては経年の差があげられ、論理部が導入開始から約１０年経過しており技術的には安定していることがあげられる。なお、いずれの処理部においても危険側の障害はなかった。

本研究においては、列車運行に繰り返し影響を及ぼす障害原因（故障）の再発の削減が重要な課題と考え、障害原因の発生頻度と障害発生時の影響度というリスクの観点から障害を分類するリスクマトリックスを新たに提案した(表１)。リスクマトリックスにおける頻度の閾値は、障害原因（故障）が過去に発生したかどうかが重要と考え、「１回」と「再発（２回以上)」とした。また、影響度に関する閾値は、列車への影響の有無とした。

表１　リスクマトリックス

| | | 故障発生頻度 | |
|---|---|---|---|
| | | １回 | 再発 |
| 影響度 | 列車運行に影響なし<br>※主に保守作業に起因 | リスク<br>クラス<br>Ⅰ | リスク<br>クラス<br>Ⅱ |
| | 列車運行に影響あり<br>※列車運行に影響を及ぼした、もしくは影響を及ぼす可能性があったもの | リスク<br>クラス<br>Ⅲ | リスク<br>クラス<br>Ⅳ |

表１にもとづき分析した結果、図４、図５に示す様に列車運行に影響する故障の再発（リスクⅣ）の割合は論理部・端末部ともに大きく、同一故障の再発防止に加えて、列車運行に対する影響防止ならびに他の設置箇所での発生防止を観点とした対策検討が重要であることを再確認できた。

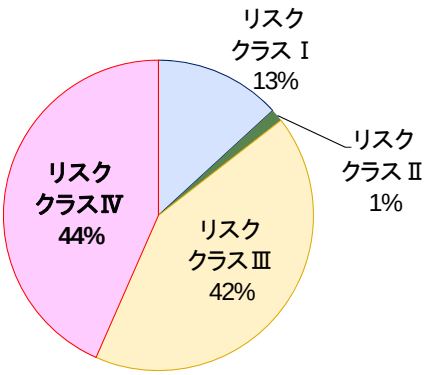


図４　リスククラスの割合（論理部）

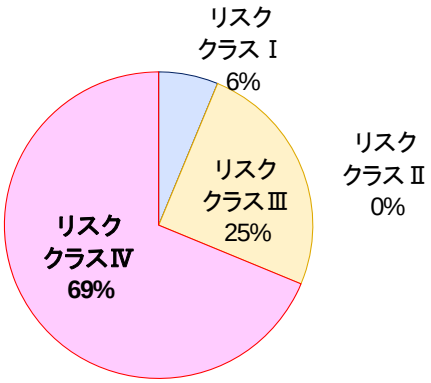


図５　リスククラスの割合（端末部）

## ４．故障データの管理手法の検討

現在、障害は障害管理表により時系列で１件ごとに管理され、確実に対処されている。しかし、ボトムアップ的な管理となるので、システム全体の観点から障害とその原因の因果関係を明確化するために、トップダウン的な解析手法である FTA を障害管理に適用することを試みた。一般に設計段階における FTA では、危険側障害として衝突・脱線、また、安全側障害としては停止現示などが頂上事象として設定され、これらの障害に至る原因が特定される。FTA 形式での障害管理

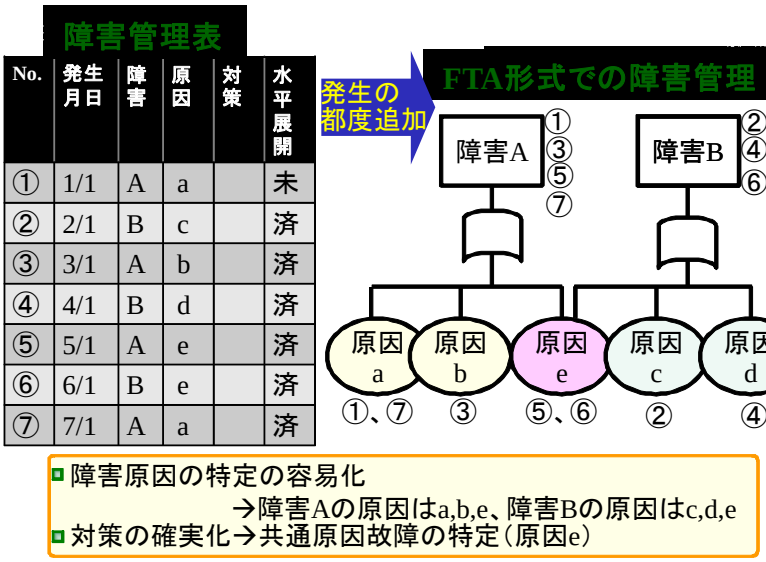


図６　FTA 形式での障害管理の考え方

においても、障害とその原因を OR 記号などで関連づけるのは同じである。相違点は、図６に示す様に障害が新たに発生した時に該当する障害もしくはその原因が無い場合に、新たに頂上事象（障害 A,B）もしくは起因事象（原因 a～e）として随時追加する点である。この様な FTA 形式での障害管理を適用することにより障害原因が一目瞭然となり、複数の障害間の共通原因故障の特定も可能になる。

FTA 形式での管理を実際に適用し、結果にもとづき障害とその原因を一覧表で管理すれば、障害原因の特定が容易になること、また、FTA 形式での障害管理は、複数の障害間の共通原因故障の特定できることを確認した。

## ５．安全性技術の再評価法の検討

リスクを観点に、システムに組み込んだ安全性技術による安全側制御の動作頻度と障害の影響低減効果から、電子連動装置に適用されている安全性技術を再評価する。図７に、安全性技術による安全側制御の動作回数、ならびに、安全側制御に至った障害原因をリスククラスで分類した結果を示す。システムに組み込まれている安全性技術の種別は障害内容から推定した。

ハードウェア故障に対する積極的な診断ならびにアプリケーションによる合理性チェックによる安全側制御の動作回数が多く、また、列車に影響した障害（リスククラスⅢ、Ⅳ）に対して動

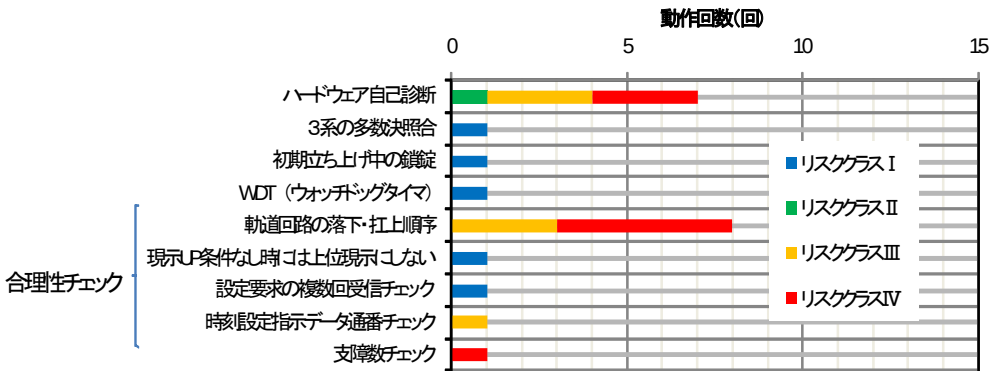


図７　安全性技術による安全側制御の動作回数（論理部抜粋）

作している割合が大きいことから、重要技術であることを再確認できた。システム開発においては、有効な技術は確実に踏襲することが重要である。

なお、安全性技術をシステムに組み込む際には、誤って安全側制御を行わない様に、適切に設計する必要がある。

## ６．安全性技術の効率的な適用

電子連動装置を対象にリスク評価した結果を踏まえ、鉄道信号装置のリスク低減に重要な項目を以下に示す。

### （１）障害発生頻度の低減

障害の発生頻度を低減するためには、システム全体の仕様を明確化し、仕様に定められた全項目に対して事前に十分試験を実施する取り組みが重要である。システムの多機能化、ネットワーク化が進展しており、設計段階におけるシステム内の全動作を必要十分な範囲で定義する取り組みが重要と考える。

### （２）障害の再発防止

障害の再発防止のためには、同一故障の再発防止だけでなく列車運行に対する影響ならびに他の設置箇所での発生防止を観点とした対策検討が重要である。重要障害の明確化には、提案リスクマトリックス（表１）が役立つ。

また、障害の再発防止策の確実化には、装置全体における個々の障害の位置づけの明確化が必要である。FTA 形式での障害管理（図６）は、障害とその原因の位置づけを明確にするとともに、新たに発生した障害原因の推定、複数の障害に共通する原因の特定に役立つ。また、列車運行に影響を及ぼしうる潜在的な障害（片系故障など）の特定にも役立つ。

### （３）安全性技術の確実な組み込み

過去の障害の再発防止には、システムに適用する安全性技術の重要性を絶えず明確にするとともに、安全性技術を確実に組み込む取り組みが重要である。その一手段としては安全性技術による安全側制御の動作実績の管理があげられる。安全性技術に関する誤動作原因を装置間で共有し、誤動作を減らす努力の継続が、システムの安全を確保しつつ安定稼動をはかる改善につながると考える。

以上の項目の実施が、鉄道信号装置への安全性技術の効率的な適用につながると考える。

## ７．おわりに

電子連動装置の障害管理表をもとに、障害原因についてリスク（障害の発生頻度とその影響度）の観点から分析し、故障データの管理手法ならびにシステムに適用されている安全性技術の再評価法を検討した。積極的なシステムのリスク管理は、システムへの安全性技術の効果的な適用につながるものであり、また、運用開始後におけるシステムの一層の安定性向上に寄与する。

また、リスク管理は、システム開発におけるライフサイクルコスト削減にもつながると考える。

## 参考文献

１）IEC 62278：Railway applications –Specification and demonstration of reliability, availability, maintainability and safety (RAMS), 2002.