鉄道信号への先端安全技術・リスクマネジメント手法の適用

鉄道信号への先端安全技術・リスクマネジメント手法の
適用に関する調査専門委員会編

（発行日　２０２４年２月７日）

目　　次

鉄道信号への先端安全技術・リスクマネジメント手法の適用に関する調査専門委員会委員

委員長	平尾　裕司	(長岡技術科学大学)
幹事	遠山　喬	(鉄道総研)
	小山　修一	(京三製作所)
幹事補佐	内田　勉	(京三製作所)
委員	中村　英夫	(日本大学)
	水間　毅	(京三製作所)
	田代　維史	(信号情報技研)
	松本　雅行	(松本信号システムコンサルタント)
	山本　正宣	(山本技術士事務所)
	川野　卓	(東日本旅客鉄道)
	前田　誠	(西日本旅客鉄道)
	岡本　誠司	(東京都交通局)
委員	大島　学	(東京地下鉄)
	澤田　和巳	(小田急電鉄)
	畑　好之	(京三製作所)
	田村　守	(三工社)
	寺田　貴行	(大同信号)
	森貞　晃	(日本信号)
	豊田　毅彦	(東芝インフラシステムズ)
	Andrew Ellison	(日立製作所)
	戸次　圭介	(日立製作所)
	石岡　卓也	(三菱電機)
途中退任	太田　正毅	(西日本旅客鉄道)

1. 総論

1.1 本調査専門委員会設置の背景

1985 年の電子連動装置の実用化に続き，ATS や ATC など多くの鉄道信号システムにもマイクロコンピュータが適用され，コンピュータ制御によって実現される機能によってこれまで鉄道信号システムは鉄道輸送システムの高度化に大きく貢献してきた。

しかしながら，このような鉄道信号システムの安全技術，リスクマネジメント手法については，十分な実績を有しているものの基本的にはほぼ 40 年前に確立されたものであり，いくつかの課題を有している。特に，今後は複数のサブシステムが複雑に結合してより高度な機能を実現するシステム構成が必要になるが，従来からのソフトウェア開発方法では FTA などによる要件分析をもとに仕様を決定しており，安全要求仕様の十分性を主張することには限界がある。また，ハードウェアについても，これまでコア間での競合による処理遅れ時間がシステムの安全許容条件を超えてマルチコア CPU が適用できなかった航空分野に新開発によって導入されようとしており，鉄道信号の分野においてもシステムの高機能化に対応するためにも安全を保証する処理部の高性能化が必要と考えられる。さらに，高機能化および構成の複雑化によって生じるセキュリティを含む新たなリスクに対しても，従来とは異なる対応が必要とされる。

新たな技術として各種分野で応用が期待されている AI については，安全確保の視点から鉄道信号システムに適用するための条件について早期の段階から詰めておくことが必要とされる。

このような状況のもとで，航空宇宙など，高機能で高い安全レベルのシステムが求められる分野で開発，適用されている先端安全技術・リスクマネジメント手法について調査するとともに，これまで実績のある鉄道信号システムにおけるこれら手法との関係を明確にし，高度な機能の鉄道信号システムに対応できる安全技術とリスクマネジメント手法の基礎を確立することを目的として，鉄道信号への先端安全技術・リスクマネジメント手法の適用に関する調査専門委員会が 2020 年 2 月に設置された。

1.2 本調査専門委員会における検討と技術報告の構成

以上のような背景のもとで設置された調査専門委員会では，高機能で高い安全レベルが求められる先端分野における AI，セキュリティ，フォーマルメソッド，ハードウェアなどに関する先端安全技術・マネジメント手法について調査を行い，鉄道信号システムに適用するための対応について考察した。

具体的な調査検討の進め方として，最初に従来の鉄道信号システムの安全技術・リスクマネジメント手法について整理し，その後に先端分野における AI，サイバーセキュリティ，フォーマルメソッド，要求事項の明確化に有効な GSN，モデルベースなどの開発手法，先端ハードウェアなどに関する安全技術・リスクマネジメント手法について調査した。さらに，これら先端分野の安全技術・リスクマネジメント手法を鉄道信号システムに適用する場合の課題とその解決アプローチについて検討するとともに，本調査専門委員会からの提言として将来への展望について議論した。

本技術報告は，このような鉄道信号システムへの先端安全技術・リスクマネジメント手法の適用に関する調査専門委員会における検討結果をまとめたものであり，5 章から構成されている。各章の概要は以下のとおりである。

第 1 章まえがきでは，調査専門委員会設置の背景と調査検討の進め方，その成果である技術報告の構成について概説している。

第 2 章従来の信号システムの安全技術・リスクマネジメント手法では，日本における従来の鉄道信号システムの安全技術・リスクマネジメント手法について，その発展経緯と現状，日本におけるものづくり文化における安全技術・マネジメント手法の特徴について論じている。日本では海外の鉄道信号システムと比較してより高い安全性と信頼性を確保してきた実績があり，RAMS（Reliability, Availability, Maintainability, Safety）の国際規格（IEC 62278）を含め新たな技術・マネジメント手法に学ぶ必要はあるものの，海外の鉄道信号システムにはない優れた対応もあり，海外の鉄道信号システムの手法との調和させるアプローチの有用性について論じている。また，第 2 章は，第 3 章以降の先端分野における安全技術・リスクマネジメント手法と鉄道信号におけるこれら手法との違いや，先端分野の手法を鉄道信号に適用を検討するうえで基礎となる。

第 3 章先端分野における新安全技術・リスクマネジメント手法では，AI に関して (a) 無人システムへの適用に関する米国国防総省のガイド，(b) セーフティシステムへの応用における課題，(c) 自律システムにおける機械学習の保証のためのガイダンス，(d) 自律システムのセーフティアシュアランスのオブジェクティブ，(e) AI 応用システムにおける透明性の考え方の調査結果が述べられている。さらに，(f) ディジタルツインの応用，(g) サイバーセキュリティ，(h) フォーマルメソッド，(i) GSN，(j) モデルベースのアプローチ，(k) STAMP/STPA，(l) MCP の新たな計 12 の先端分野での新たな安全技術・リスクマネジメント手法について調査結果を述べている。

第 4 章先端分野の安全技術・リスクマネジメント手法の鉄道信号システムへの適用では，第 3 章で調査した計 12 の手法を鉄道信号システムに適用するための課題とその解決のためのアプローチについて，(a) AI，(b) ディジタルツイン，(c) サイバーセキュリティ，(d) フォーマルメソッド，(e) GSN，(f) RCA，(g) STAMP/STPA，(h) 安全処理部ハードウェアアーキテクチャの共通化に集約して論じている。