⑨ 交通システムの車両・設備に関わる安全性評価の標準化について

交通システム研究領域　※林田 守正　廣瀬 道雄　吉永 純　長谷川 智紀　工藤 希

1．はじめに

わが国における軌道系交通システム、およびその車両、設備に関わる技術評価は、国が定める技術基準に準拠するだけでなく、鉄道事業者独自の考えで行われてきた。また安全性については、わが国の鉄道の長年にわたる極めて高度な安全の実績を背景とした評価が行われてきた。しかし急速な国際化の流れの中で、従来わが国には馴染みが薄かった RAMS や数値管理等の概念に基づく国際規格が成立するようになってきた。本報告では、これまで交通安全環境研究所（以下「当所」という）による車両・設備に関する安全性評価を総括し、国際規格との整合を前提とした評価手法の標準化について述べる。

2．交通安全環境研究所による安全性評価

2．1　これまでの経緯

当所は、これまで公正中立な第三者機関（以下「第三者」という）として、先進的な公共交通システムの実用化、あるいは新技術の導入に際して、各分野や段階における安全性評価を実施してきた。その事例を表1に示す。青字は 2000 年以前、赤字はそれ以降の評価事例である。

鉄道事業者が既存システムの改良や海外製品の導入を行う際には、所管の運輸局への届出と、それに先立つ安全性の証明が必要となる場合がある。また、全く新しいシステムや技術が導入される際は、開発段階から国土交通省鉄道局がオブザーバ参加し、評価は委員会または第三者が行うケースがある。当所は第三者の一つとして、従来は主にこのような国内向けの安全性評価に携わってきた。これらの安全性評価は主に国内の鉄道事業を対象とするものであり、長年にわたって培われたわが国の鉄道システムの高水準な安全性の実績を背景とし、国際規格を参照、考慮しながらも、国内技術基準への適合や従来と同等以上の安全性の確保を主眼とした評価を行ってきた。

表1　交通安全環境研究所が実施してきた安全性評価事例（索道関係・事故調査は含まない）

	開発段階		実用段階		技術基準、標準仕様策定、評価手法検討に相当するもの
	設計のみ	試作車両・機器あり（単体、試験線による試験）	運用開始前（実路線での走行試験等）	運用後の改良等	
全体システム（車両・軌道・信号）		・新交通システム ・常電動磁気浮上鉄道 ・リニア地下鉄 ・IMTS（バス型磁気誘導鉄道） ・外国製ゴムタイヤトラム ・ｺｰｽﾀｰ型軽量軌道ｼｽﾃﾑ ・各種新方式交通システム *海外向けLRT	・アプト式鉄道 ・ガイドウェイバス ・国内空港APM ・ロープ駆動式モノレール ・LRT	・都市鉄道速度向上 ・勾配区間の駅停車 ・ローカル鉄道速度向上	・ガイドウェイバス ・常伝導磁気浮上鉄道 ・地上一次ﾘﾆｱ試験装置 ・IMTS ・安全性の定量的評価法 ・外国製ゴムタイヤトラム ・ｺｰｽﾀｰ型軽量軌道ｼｽﾃﾑ
車両	・小径車輪付LRV用ブレーキ *新交通車両ﾌﾞﾚｰｷ制御ﾕﾆｯﾄ	・一軸台車 ・軌間可変台車 ・独立回転車輪付LRV ・各種操舵台車 ・新交通ｼｽﾃﾑ用新方式台車	・海外技術超低床LRV	・車両検査周期見直し ・新規車両導入 ・LRV付属品改良	・VVVFｲﾝﾊﾞｰﾀのﾌﾞﾚｰｷ制御 ・地上一次ﾘﾆｱﾓｰﾀｰ保安設備 ・車両検査周期見直し ・試験、測定国際標準化動向
軌道／構造物				・レール波状摩耗対策 ・ﾘﾆｱ地下鉄ﾘｱｸｼｮﾝﾌﾟﾚｰﾄ改良	・ﾌﾟﾛｰﾌﾞ車両ｼｽﾃﾑ ・地上輪重／横圧測定法 ・脱線係数の常時観測
機械設備／電力		・モノレール給電線配置変更 ・ホーム可動ステップ	・海外技術LRT用新型軌道 ・輸入摩擦型終端車止め		
信号保安／列車制御システム	・改良版電子連動装置 *空港内APM用列車制御ｼｽﾃﾑ *高速鉄道用空間波方式CBTC *無線測距方式CBTC *近接通信方式CBTC *CBTCソフトウェア基本構造 *車軸検知装置 *電子連動装置輸出先対応 *電子連動装置機能付加	・常伝導磁気浮上鉄道速度計 ・次世代障害物検知システム ・衛星利用ATP閉塞システム ・民鉄向高機能ATS ・民鉄向ATC ・車載型画像解析応用地上設備予防保全ｼｽﾃﾑ（当所開発）	・輸入LRT用信号保安ｼｽﾃﾑ *海外高速鉄道路線信号ｼｽﾃﾑ	・踏切制御システム改良	・特殊自動閉塞システム ・無絶縁軌道回路 ・ATC模擬試験 ・衛星測位利用運行管理 ・CBTC
EMC		・常伝導磁気浮上鉄道漏洩磁界	・鉄道車両からの漏洩磁界	・実車ﾌｨﾙﾀﾘｱｸﾄﾙ用遮蔽材	・磁界測定法 ・磁界影響評価 ・交流磁界遮蔽 ・ﾘﾆｱﾓｰﾀ鉄道からの漏洩磁界 ・鉄道の磁界に対するEMC

注）LRV：次世代型路面電車　LRT：次世代型路面電車システム　CBTC：無線式列車制御システム　APM：自動運転ゴムタイヤ式輸送システム　EMC：電磁界影響両立性

２．２．海外案件の増加

近年、国内メーカによる自社製品の海外展開が活発化し、その際に、国際規格への適合性を要求され、また第三者による認証や安全性評価が必要とされるケースが増加してきた。一方、国内の鉄道事業者は主に国内メーカから調達を行ってきたが、一部ではWTO協定により調達先の海外への開放が義務付けられ、仕様は国際規格に準拠することが求められるような例も増加しつつある。当所の安全性評価も表１に示すように海外案件が増加しており、中でも信号保安システムの設計段階での事前安全性評価が多くを占めるようになっている。従って国内技術の海外展開、および海外技術の導入の両面から、国際規格との整合性を考慮した安全性評価手法の標準化が必要となっている。

３．安全性評価の要点

３．１．鉄道の安全の確保と技術の変遷

一般に、信号保安システムの安全を確保するためにはフェールセーフ性の確保が重要視されてきた。フェールセーフの確保とは、壊れても安全側（停止）に動作するよう設計することである。しかし、近年では、信頼性の確保も重要な視点となり、安全確保の考え方に、予防安全の考え方も取り込まれるようになってきた。予防安全とは、壊れる前に検知して安全側に制御することであるが、これは必ずしも列車を停止させることだけではなく、保守時に部品交換等を行って営業に差し支えないようにすることも含まれる[(1)(2)]。

すなわち、フェールセーフは、古くから鉄道の安全の基本であり、例えば信号保安装置に多用されてきたリレーの場合、故障や停電の際は機構的に電源が切れる側に機能し、本質的に、システムの危険側動作を防止する構成を取ってきた[(2)]。また予防安全は、状態監視システムにより機器状態の変化を検知して故障に至る前に、安全側に制御することを前提として交換を指示する等、未然に故障を防止して、安全性だけでなく信頼性も確保する考え方である。ただし、こうした予防安全技術が本質的に安全かどうかを評価しなければならない。

一方、エレクトロニクス技術の飛躍的な発展に伴い、安全技術もハードウェアからソフトウェアへ、アナログからディジタルへ、有線通信から無線通信へ、地上主体から車上主体へと、安全を確保しつつ省コスト化を図る方向性が主流となっている[(1)]。特に鉄道の安全の要となる信号保安システムで、電子部品等を多用した電子連動装置やディジタル ATC 等においては、多重化やソフトウェアによるフェールセーフ性を持たせ、さらに最近開発が進んでいる図１のような無線式列車制御システム（CBTC）ではソフトウェアと無線によるフェールセーフ性を担保するような設計となっている[(1)]。したがって、こうしたシステム、技術の評価が重要となってきている。

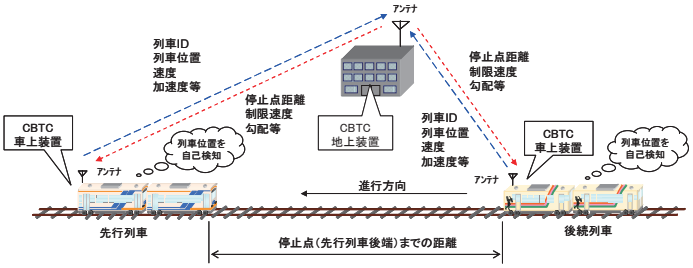

図１　無線式列車制御システムの概念

３．２．フェールセーフ性の証明

安全技術の評価とは、安全を確保する技術がどの程度安全かを証明することである。安全技術の評価とは、安全技術が本当に安全か、どのように安全であることを証明するか、という点である。日本では、その指標を数値ではなく、これまでの日本の鉄道と同等程度の安全を確保するということで評価してきた。図２に従来の信号保安（従来タイプ）と新しい概念の信号保安(新タイプ)に対する安全性評価の要点を示す[(2)]。

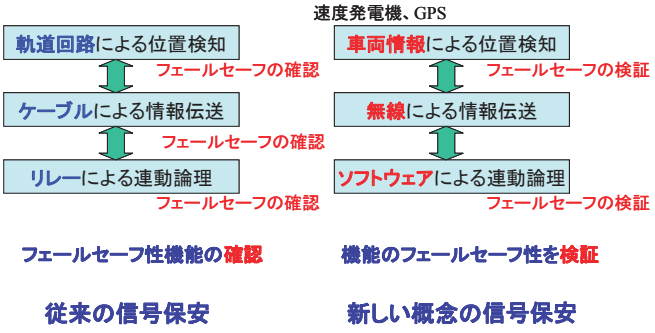

図２　信号保安のフェールセーフ性の評価[(2)]

本質的にフェールセーフである軌道回路やリレー等で構成され、長年の実績がある従来タイプでは、各々の機能のフェールセーフ性を確認することが評価の主体である。この評価では、従来並の安全性を確保することがフェールセーフ性を証明することとなる。一方、人手が介在するソフトウェアや、データ化けや接続断のリスクを本質的に持つ無線を使う論理で構成される新タイプでは、各機能のフェールセーフ

性を証明し検証する必要がある[2]。ここでは、従来と同等の安全性を確保するといった議論が難しく、ヨーロッパ流の数値（SIL：安全性インテグリティレベル）の考え方も取り入れざるを得なくなっている。

3．3．FTA、FMEAによる検証

機能のフェールセーフ性の検証の主要な手法として、国内外でFMEA（Failure Mode and Effects Analysis）およびFTA（Fault Tree Analysis）が多用されている。FMEAは各機器、装置、モジュールの故障モードを抽出し、その影響と対策を評価するボトムアップ的な手法である。数値化された故障による危害の重大さ（ハザードレベル）と発生頻度を乗算してリスク評価を行い、設定した閾値以下となるよう対応する。図3にFMEAの例を示す[1][2]。一方、FTAは重大な異常事象（ハザード）を抽出し、その下位事象と対策（制約ゲート）を評価するトップダウン的な手法である。図3にFTAの一例を示す[1]。

表2　FMEAの一例[1][2]

対象		故障モード	想定原因	影響範囲	故障検出	安全性確保	ハザードレベル	発生頻度
信号保安システム	GPS	電源故障	断線、劣化、素子異常等	GPS受信器、位置情報処理装置等	信号処理部	停止指令、他系による縮退モード走行	Ⅱ	2
		GPS故障	電波受信異常GPS素子故障	位置検知	信号処理部	他系システムとの比較により、停止指令	Ⅱ	3
	信号処理部	処理部故障	電圧低下、ノイズ、断線等	システム全体動作	出力リレー	FSCPUによる検出、リレーによるフェールセーフ性確保	Ⅲ	2
		通信部故障	電圧低下、ノイズ、断線等	通信不能	信号処理部	停止指令、	Ⅲ	1
	速度取得装置	処理部故障	電圧低下、ノイズ、断線等	速度検出不能	信号処理部	速度データ妥当性判断、正常系による縮退モード走行	Ⅱ	1
		通信部故障	電圧低下、ノイズ、断線等	通信不能	信号処理部	停止指令	Ⅲ	2
汎用通信システム	通信部	通信部故障	断線、電圧低下等	通信不能	信号処理部	停止指令	Ⅲ	1
		通信異常	ノイズ、電波障害等	通信異常（見かけ上の通信は可能）	信号処理	情報の妥当性判断、異常と判定すれば停止指令	Ⅲ or Ⅳ	2

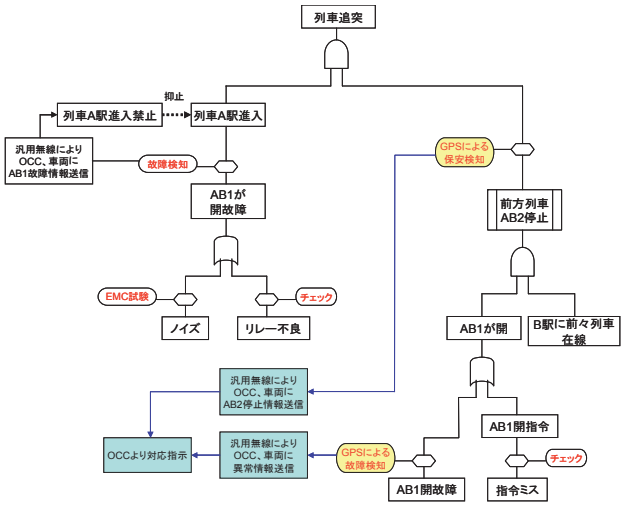

図3　FTAの一例[1][2]

当所ではFMEAの実施により最悪事象を特定し、その最悪事象をTOP事象とするFTAを実施している。さらに必要に応じてETAや状態遷移図を活用して、故障確率の算定も行っている。このような手法によって、評価対象の安全性を数値的に評価して、システムのフェールセーフ性を証明している。ヨーロッパの考え方では、フェールセーフ性は、SIL4（1要素当たりの危険事象発生確率が 10^{-8}～10^{-9}/hr）を確保すれば良いこととなっているが、当所では、従来システムと同等以上の安全性を数値化して、それを確保しているか否かの観点で評価を行ってきた。

4．安全性評価の国際規格との整合

4．1．鉄道の安全に関する国際規格

鉄道に関する主要な国際規格としては、表3に示すように、電気系ではIEC（国際電気標準会議）規格、機械系ではISO（国際標準化機構）規格が挙げられる。IECには鉄道分野の専門委員会TC9が設置され、効率的な審議が行われている。その中で、IEC62278（RAMS）は鉄道の構成要素全般を対象としており、安全性に関して、その目標設定から維持まで、ライフサイクルの各段毎に実施事項を規定している。またIEC62425はIEC62278の安全性証明手続き（セーフティケース）を詳細に規定している。一方、ISOにおいても新たに鉄道専門委員会TC269の設立が決定され、機械系の国際規格化が活発化していく可能性がある[3]。

表3　鉄道の安全に関する主な国際規格

規格番号	規格の概要
IEC61508-1～7	安全に関連する電気/電子/ﾌﾟﾛｸﾞﾗﾏﾌﾞﾙ電子装置（全産業）
IEC 62278	鉄道におけるRAMS
IEC 62425	鉄道信号用安全関連電子装置の安全性証明（セーフティケース）
IEC 62279	鉄道信号システムのソフトウェアの安全性
IEC 62280	鉄道信号システムの通信の安全性
IEC 62236	鉄道システムのEMC

4．2．国際規格との整合に向けた課題

4．2．1．リスクの数値管理と妥当性

国際規格においては、IEC61508-1等により安全性インテグリティレベル（SIL）が数値で定義されている。またIEC62278には社会的に受け入れ可能な許容リスクの原則について以下のように記述されている[4]。

・ALARP（英）：現実的に実現可能な限り低いこと
・GAMAB（仏）：少なくとも既存ｼｽﾃﾑと同等の安全性
・MEM（独）：死亡事故のリスクが最も少ないこと

これらはリスクを数値管理するという考え方で、安全性の評価を閾値によって判断するものである。これ

に対して、日本では、鉄道事故を限りなくゼロにするという考え方が一般的であると思われる。

ただし、わが国の鉄道は設計上も実績でも、上記のSIL4 や欧州規定より桁違いに高い安全性を実現している。したがって当所では、計算上の確率を求めるとともに、SIL に拘らずに、日本の鉄道の安全性の実績と比較・評価することで、高水準の安全性を担保するという考えである。

４．２．２．IEC62278（RAMS）との整合

IEC62278 が規定する RAMS は、適用対象システムが、信頼性(Reliability)、可用性(Availability)、保守性(Maintenance)、安全性(Safety)を総合的かつ良好なバランスで維持することを要求する規格である。RAMS のライフサイクルは、図 4 に示すように 14 段階に分かれる。表 1 に示した安全性評価案件のうち、わが国の鉄道技術の海外展開を主眼とした開発段階、特に信号保安／列車制御システムの設計段階における評価は、主に第 1 段階から第 7 段階までに含まれると考えられる。

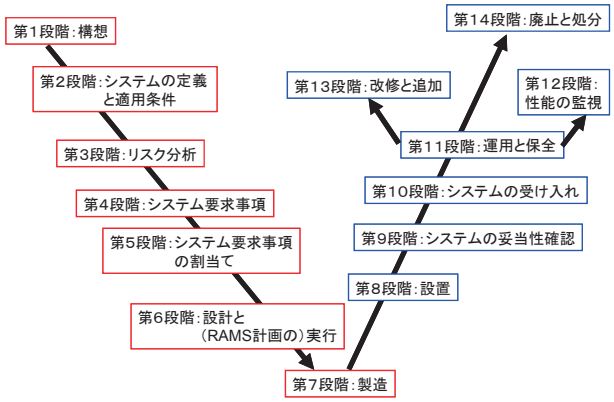

図 4　RAMS に示されるライフサイクルの 14 段階 [4]

IEC62278 には、安全性（RAMS の S）の技術的な概念形成の基となるハザード、リスク等の概念が定義され、図 4 の各段階における安全性業務が定められている [4]。そのため第三者による安全性評価を IEC62278 と整合させるためには、上記の概念や定義を踏まえ、RAMS 各段階に定められた安全性業務と、評価の手順や結果との対応が明確であることが必要と考える。特に第 3 段階でのリスク分析は、場合により他の段階でも繰り返す必要性が示唆されているため、前述の FMEA、FTA も、対象とする段階を明確にする必要がある。また第6段階で作成が義務付けられている総合セーフティケース（信号用安全関連電子装置については IEC62425 で規定）は、安全性要求事項に適合することを証明するものであるため、それに含まれるべき諸事項と、安全性評価結果の内容との対応が重要であると考えられる。

これに対し、従来のわが国における設計においては、包括的には RAMS の内容をほぼ満たしており、トータルの安全性は、規格で規定されている SIL4 以上を実現しているものの、ここで規定されているようなプロセスを手順通り実行しているとは言い難い部分もあった。したがって、今後、国際規格への適合を求められた場合は、手順通りのプロセスの実施、適切な文書管理を含めた安全性評価が求められると考える。

４．２．３．その他の国際規格との整合

IEC 規格としては RAMS 以外にもソフトウェア、通信、EMC 等に関する規格と安全性評価との整合は重要である。また多くの IEC 規格の母体となった EN 規格（欧州統一規格）との整合を要求されるケースも見られ、一方、今後は整備が進んでいく鉄道関係の ISO 規格への整合も求められることが予想される。

５．鉄道認証との関係

これまでは、国内に鉄道認証機関が存在しなかったため、安全性評価が「認証に代わるもの」として求められるケースもあった。今後は安全性評価が認証前の過程として必要とされる場合も含め、その結果が海外にも受け入れられるように、国際規格との整合を図りながら手法の標準化を図っていく必要がある。

６．まとめ

(1) 交通安全環境研究所が取り組んできた鉄道技術に関する安全性評価の経緯と現況を総括した。

(2) 鉄道の安全性に関連する国際規格と整合への課題を整理し、わが国の鉄道技術の海外展開に資する安全性評価手法の標準化の方向性を提案した。

［参考文献］

1) 水間：安全技術のチェンジ、平成 21 年電気学会産業応用部門大会前刷集 Ⅲ-143～146（2009）

2) 水間：鉄道における安全技術と FMEA, FTA、交通安全環境研究所研修資料（2012）

3) 田中：鉄道分野の国際標準化活動の動向と日本の取り組み、第 258 回鉄道総合技術研究所月例発表会前刷集（2012）

4) IEC62278 第一版 英和対訳版 、日本規格協会(2002)