講演３．RAMS を考慮した鉄道技術の標準的な第三者安全性評価手法に関する取組

交通システム研究部　※林田 守正　佐藤 安弘　大野 寛之　工藤 希
元交通システム研究部　廣瀬 道雄
東京大学　水間 毅

１．はじめに

交通安全環境研究所（当研究所）は鉄道技術に関する第三者機関としての安全性評価（以下、第三者安全性評価）に数多く取り組んできた。一方で、国際規格 IEC 62278 において「信頼性(R)・アベイラビリティ(A)・保全性(M)・安全性(S)」（RAMS）が定義されたことにより [1]、これまでの安全性評価に RAMS の概念を取り入れる必要が生じている。そのため、当研究所では安全性(S) だけでなく信頼性等 (RAM) の評価についても検討することにより、高い安全性の担保に加え、RAM を考慮した標準的な第三者安全性評価手法の構築に向けた取組を行っている。その内容について、昨年度に引き続いて報告する。

２．第三者安全性評価の位置付け

２．１．鉄道技術の国際化への対応について

当研究所は、これまで公正中立な立場から、先進的な交通システムの実用化、あるいは新技術の導入やシステム改良に際して、各分野／段階における第三者安全性評価を実施してきた。わが国の鉄道技術は極めて高い安全性を有しているものの、鉄道製品の国際展開に当たっては、外国の技術基準や IEC シリーズ等の国際規格群への適合が重要となっている [2]。当研究所の第三者安全性評価も、国際規格等との整合が必要とされる海外向けシステムの設計安全性を対象とする事例が増加しており、その形態の推移を図１に示す。

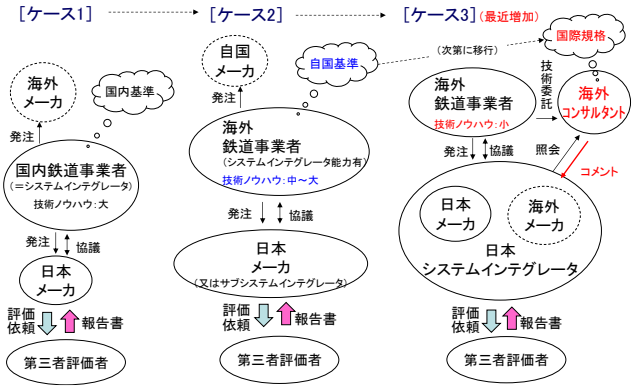

図１　第三者安全性評価の形態の推移

２．２．RAMS の概念

IEC 62278 においては、安全性(S)だけでなく信頼性等（RAM）を含めた総合的な評価項目として、RAMS が表１のとおり定義されている [1]。RAMS の概念に基づく技術評価の検討例は幾つか見られるが [3]、本研究では、安全性(S)と RAM のバランスを考慮した第三者安全性評価の標準的な手法を検討している。

表１　RAMS の定義 [1]

項目	IEC62278における定義
信頼性 (R)	アイテムが、所定の条件と所定の時間間隔(t1,t2)で要求された機能を果たし得る確率。
アベイラビリティ(A)	外部から必要な資源の供給を行えば要求機能を所定の時間又は期間中、所定の条件において果たし得る状態を維持することができる製品の能力。
保全性 (M)	所定の手順と資源を使って所定の条件でメンテナンスを行う場合に、所定の条件で使用されているアイテムを所定の期間内にメンテナンスすることができる可能性。
安全性 (S)	許容出来ない危害が発生するリスクが無いこと。

２．３．第三者安全性評価と規格適合性評価／認証

鉄道製品の機能安全に関する国際規格への適合性を示す手段としては、第三者機関による規格適合性評価／認証を受けることが最も一般的である [2]。当研究所においては、鉄道認証室が認証機関として、機能安全規格である IEC 62278 や IEC 62425 [4]等について規格適合性評価／認証を担当している。一方、交通システム研究部が担当している第三者安全性評価の報告書は、海外鉄道事業者等の相手先の判断により、認証書に代わる機能安全の証拠として活用される場合もある [2]。

表２　第三者安全性評価と規格適合性評価／認証

	第三者安全性評価 （主に設計安全性）	国際規格適合性評価／認証 （機能安全関連）
評価の対象	・製品の技術内容、設計仕様等	・製品に対する安全マネジメントのプロセス
評価の主眼	・SIL等の指標に沿ったリスク分析に基づいた定量的な評価。 ・システムの安全管理にかかわる定性的な評価.	・各種証拠文書の記述の対象国際規格（IEC等）各条文に対する適合性の確認。
IEC 62278 RAMS 14段階への対応範囲	・主に第6段階まで	・主に第7段階まで
国際展開において第三者評価が活用されるケース[2]	・国際規格適合性評価／認証に代わるものとして要求される場合（相手先が安全性評価報告書を認証書相当と判断することが前提）。 ・規格適合性の証拠文書の一部として安全性評価報告書が要求される場合（規格適合性評価／認証を並行して実施）。	・機能安全に関する国際規格への適合の証拠を要求される場合。
評価機関としてのオーソライズ	・国際的なオーソライズの仕組みは特に無い。	・認証機関に対する要求事項が国際規格（ISO/IEC 17065）で定められている。 ・認定機関による認定を取得している。

当研究所の第三者安全性評価と規格適合性評価／認証の比較を表 2 に示す。安全性評価では技術的な内容や仕様を対象として、SIL（Safety Integrity Level）[1]等の指標に沿って、リスク分析に基づいた定量的評価やシステムの安全管理にかかわる定性的な評価などを行うことが主眼となる。規格適合性評価では、安全マネジメントのプロセスの結果である各種証拠文書を確認することが主眼となる[2]。設計安全性評価では、RAMS の 14 段階[1]のうち第 6 段階（設計と実行）までを主な対象範囲と考えている。なお IEC 62425 では、システムの安全性承認には Safety Case と第三者安全性評価（ISA：Independent Safety Assessment）が必須とされる[3]。ここでは「ISA」は安全性評価を意味するか、または機能安全規格適合性評価／認証を意味するかは明確にされていないが、当研究所の第三者安全性評価結果（報告書）は、図 2 に示すように Safety Case 第 4 部「Technical Safety Report」に記述される安全性の証拠に該当すると解釈できる。

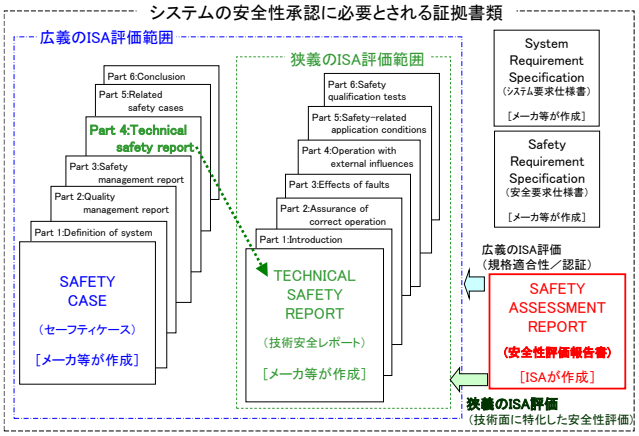

図 2　IEC 62425 における第三者安全性評価の解釈

3．RAMS への対応について

3．1．RAM の評価パラメータ

IEC 62278 には、鉄道分野への利用に適するとされる RAMS のパラメータが例示されている。その一部を表 3 に示す[1]。信頼性（R）のパラメータとしては故障率（頻度）、平均故障間隔、信頼度等、従来からわが国においても一般的に使用されているものが含まれている。アベイラビリティ（A）、保全性（M）についても同様である。なお安全性（S）のパラメータの 1 つとしてハザード率が挙げられているが、これは信頼性のパラメータである故障率のうち「危険側故障率」に相当し、IEC 61508 では「時間当たり危険側故障平均頻度」（PFH）として定義されている[5]。危険側故障率は当研究所による第三者安全性評価においても主要なパラメータとして採用されてきた。これらの点から、RAM の評価パラメータとしては、IEC 62278 等にも記載されている故障率等の一般的なパラメータを優先的に使用することが望ましいと考える。

表 3　IEC 62278 に示されるパラメータ（一部）[1]

RAMS項目	パラメータ	記号	単位
信頼性（R）	故障率	λ	1/hr
	平均稼働時間	MUT	hr
	平均故障時間（非修理系）	MTTF	hr
	平均故障間隔（修理系）	MTBF	hr
	信頼度	R(t)	単位無し
	不信頼度	F(t)	単位無し
アベイラビリティ（A）	アベイラビリティ	A（＝MUT/(MUT+MDT)）	単位無し
保全性（M）	平均ダウン時間	MDT	hr
	平均修復時間	MTTR	hr
安全性（S）	ハザード率（危険側故障率）	H(t)	1/hr
	平均危険側故障間隔	MTBF(H)	hr

3．2．RAM のリスク評価

安全性のリスクについては、IEC 62278 に離散化した危険事象の深刻さと発生頻度の積によるマトリクス評価手法が例示されている[1]。一方、RAM のリスクについては、IEC/TR 62278-4 にマトリクス評価手法が表 4 のように例示されている[6]。故障の頻度はハザードの頻度と同様に 6 段階に区分され、影響度は、運行、快適性、保全のそれぞれの観点毎に 3 段階に区分される。それらの積であるリスクは、安全性と同様に 4 段階に区分される。RAM のリスク評価は、このような手法で行うことが望ましいと考える。

表 4　RAM のリスク評価マトリクス[6]

		影響度		
		軽度	中程度	重大
発生頻度	頻繁に発生	望ましくない	許容できない	許容できない
	発生の可能性大	許容できる	望ましくない	許容できない
	時として発生	許容できる	望ましくない	望ましくない
	いつか発生	無視できる	許容できる	望ましくない
	発生しそうもない	無視できる	無視できる	許容できる
	発生は考えられない	無視できる	無視できる	無視できる

3．3．安全性(S)と RAM のバランス

IEC 62278 には、RAMS の各項目の重み付けに関しては特に記述されていない。安全性については要求水準に関する認識が国際的にも概ね共有され、評価の尺度はある程度定まっていると考えられる。例えば、列車制御システムには SIL4 相当のレベルが要求される[7]。これに対し、RAM の要求水準は鉄道事業者等の自主的な判断に任される部分が大きい。したがって第三者安

全性評価においては､RAMS の各項目を均等に評価するのではなく、あくまでも安全性を主眼とする。一方、RAM については、それ自体の良否よりも、安全性担保の前提とするシステム要求仕様として確認する形とすることが望ましいと考える。

４．FTA による解析について

４．1. FTA による定量的解析に関する考察

当研究所の安全性評価においては、リスク分析として FMEA（Failure Mode and Effects Analysis）の結果から選定した危険事象をトップ事象とする図 3 に示すような FTA（Fault Tree Analysis）を行い、そのトップ事象が発生する確率または頻度が充分に小さいことを確認してきた。個別の基本事象（各要素の危険側故障等）の発生確率または頻度を全て特定するのは煩雑であるため、上位事象への遷移を阻む制約ゲートの条件の機能や信頼性に着目した定量的な解析を行ってきた。なお、危険側に限定しない不具合をトップ事象や基本事象とする解析は、FTA による信頼性の解析となる。

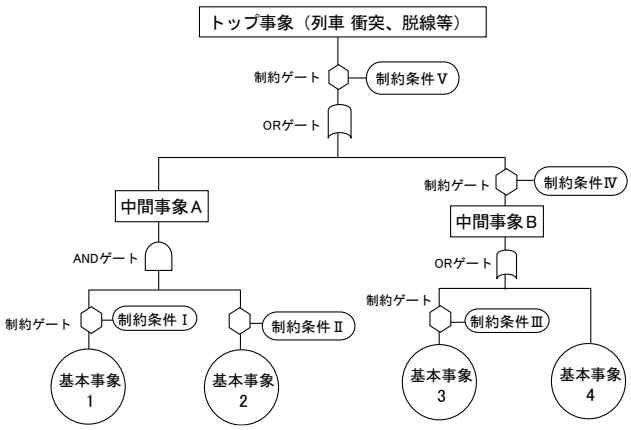

図 3　FTA の模式図

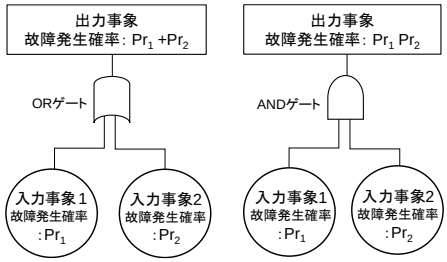

図 4　故障発生確率による解析モデル [8)]

FTA の定量的な解析手法としては､故障発生確率(無次元）による解析と、故障率（頻度、単位：1/h）による解析手法がある [8)]。ここで FTA の一部として、2 つの入力事象が OR ゲートまたは AND ゲートを介して 1 つの出力事象に至る単純なモデルを想定する。発生確率による解析においては、図 4 に示すように、OR ゲートの出力事象の発生確率は近似的に各入力事象の故障発生確率（Pr_1、Pr_2 とする）の和（$=Pr_1+Pr_2$）となり、AND ゲート上の出力事象の発生確率は各入力事象の発生確率の積（$=Pr_1 \cdot Pr_2$）となる [8)]。一方、故障率による解析においては、図 5 に示すように、OR ゲートの出力事象の故障率は、各入力事象の故障率（λ_1、λ_2 とする）の和（$=\lambda_1+\lambda_2$）となる。しかし AND ゲートの出力事象の故障率は各入力事象の故障率の積とはならず、また各故障率が一定でも経過時間 t（単位：h）の関数（$=2\lambda_1 \cdot \lambda_2 \cdot t$）となる [8)]。

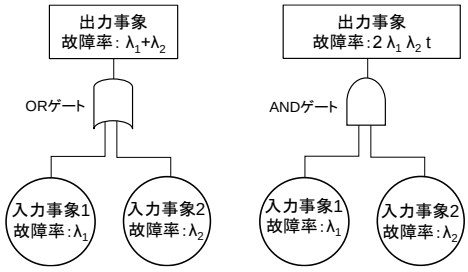

図 5　故障率による解析モデル [8)]

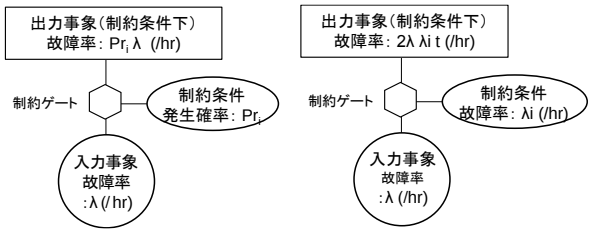

図 6　制約ゲートの条件と入出力事象の故障率 [8)]

このように故障率による解析は計算がやや複雑になるが、IEC 61508 や IEC 62425 では、鉄道の安全関連機能の SIL について、高頻度作動モードまたは連続モードでの運用への要求として、危険側故障の平均頻度（単位：1/h）として定義されている [4) 5)]。これは危険側故障率に相当するため、標準的な安全性評価手法としては故障率による FTA 解析が望ましく、経過時間 t としてはシステムの稼働期間（例えば 20 年間≒1.75×10^5 h）等を採用できると考える。なお制約ゲートは AND ゲートの変形であるが [8)]、その制約条件の定義としては前述のように、「機能しない確率」と「機能自体の故障率」の 2 通りが考えられる。それらの場合の入力事象と出力事象の故障率との関係を図 6 に示す。制約条件を故障率として定義する場合は計算が一層複雑化するが、制約ゲートとしての SIL を設定す

ることによりトップ事象の要求 SIL を担保することが容易になると考える。

４．２．信頼性解析ソフトウェアの活用

当研究所ではこれまで FMEA や FTA による解析には汎用表計算ソフトウェア等をベースとした手作業による手法（従来手法）を用いてきたが、新たに市販の信頼性解析専用ソフトウェアを活用する手法（ソフトウェア手法）を検討した。信頼性解析機能、FMEA 機能モジュールに続き、新たに FTA 機能をモジュールとして導入した。これは FMEA の結果から FTA 図を自動作成し、さらに自在な編集が可能なものである。その実行例を図 7 に示す。従来手法に対するソフトウェア手法の特長としては、階層構造の解析やトレーサビリティの確保の他、前述した故障率による FTA 解析において必要な複雑な計算が容易に行える点が挙げられる。

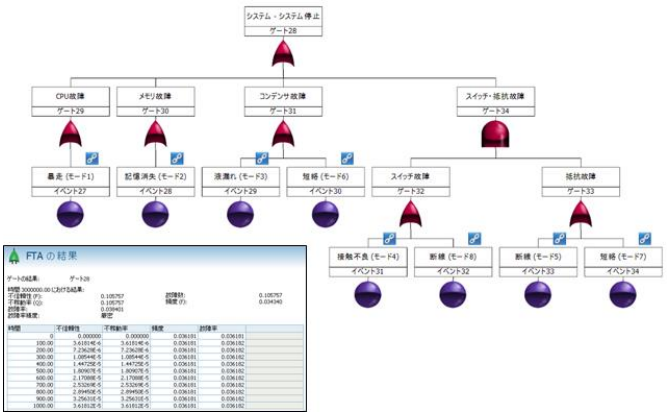

図 7　ソフトウェア手法による FTA の実行例

５．標準的な第三者安全性評価手法の構築に向けて

安全性(S)を主眼とし、RAM も考慮した標準的な第三者安全性評価報告書の内容を以下の通り検討中である。その基本構成案を図 8 に示す。

５．１．前段

緒言、評価対象範囲、評価参照資料一覧、参照国際規格、評価対象システム概要等を記述する。

５．２．評価結果

５．２．１　安全性の評価結果　以下を記述する。

・安全性に関連する技術的な要点と評価
・FMEA／FTA によるフォールトの影響解析
・実機/実車試験による FTA 結果等の検証

５．２．２　RAM の評価結果　以下を記述する

・RAM に関連する技術的な要点と評価
・MTBF、MTTR 等による数値評価
・信頼性の観点からの FMEA と FTA
・実機試験による信頼性予測の検証
・安全性と信頼性の両立に関する課題の整理

５．３．評価の結論

安全性、信頼性等に関する評価結果をまとめ、システムに要求される安全性が、所定の RAM の設定条件下で担保されるかどうかの判断を記述する。

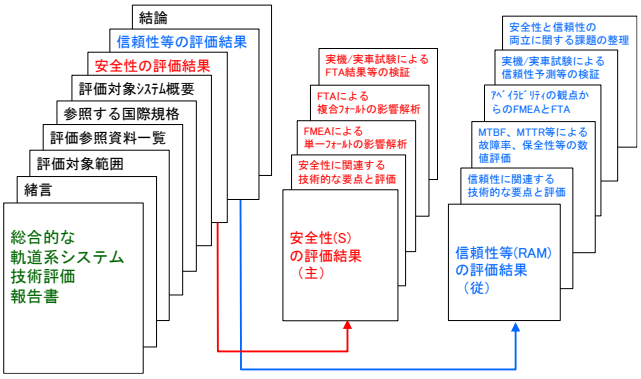

図 8　標準的な第三者安全性評価報告書の構成（案）

６．まとめ

(1)第三者安全性評価の位置付けについて国際規格や規格適合性評価／認証との関連を含めて整理した。
(2)IEC 62278 で定義される RAMS における信頼性等(RAM)のパラメータやリスク評価に関し検討した。
(3)FTA による定量的解析の課題を考察するとともに、信頼性解析ソフトウェアの FTA モジュールを導入し、試行した。
(4)RAMS を考慮した標準的な第三者安全性評価手法の構築に向け、報告書の基本構成案を提示した。

参考文献

1) IEC 62278 First edition 2002-09 英和対訳版
2) 長谷川他, "国際規格への適合性評価と交通研の果たす役割", 交通研フォーラム 2010 講演概要 pp. 114-119
3) 平栗, "RAMS の考え方に基づいて信号システムを評価する", RRR Vol.69 No.8 pp.43-52 (2012)
4) IEC 62425 Edition 1.0 2007-09
5) IEC 61508-1 Edition 2.0 2010-04 英和対訳版
6) IEC/TR 62278-4 Edition 1.0 2016-12
7) 平尾, "鉄道システムにおけるリスクベース安全管理", 日本信頼性学会誌「信頼性」Vol.33 No.8 pp.366-369 (2011)
8) 小野寺, "国際化時代の実践 FTA 手法", 日科技連出版社 pp.77-87 (2000)