講演１．軌道系交通システムの国際展開に対応した技術評価手法の検討

交通システム研究領域　　※林田 守正　　廣瀬 道雄　　大野 寛之　　森 裕貴
理事　　水間 毅

１．はじめに

日本の軌道系交通システム（鉄道等）の海外展開に際しては、国際規格に準拠した第三者安全性評価（以下「ISA（Independent Safety Assessor）評価」という）が必須とされるケースが増加している[1)]。このような状況に鑑み、国際規格の客観性や合理性と整合しつつ、これまで交通安全環境研究所（以下「当所」という）が培ってきたFMEA（Failure Mode and Effects Analysis）、FTA（Fault Tree Analysis）を中核とする手順を継承した標準的な安全性評価手法について検討した。本報ではそれを取りまとめた結果を報告し、安全性重視を堅持しつつ信頼性等も考慮した技術評価手法の確立に向けた取り組みについて述べる。

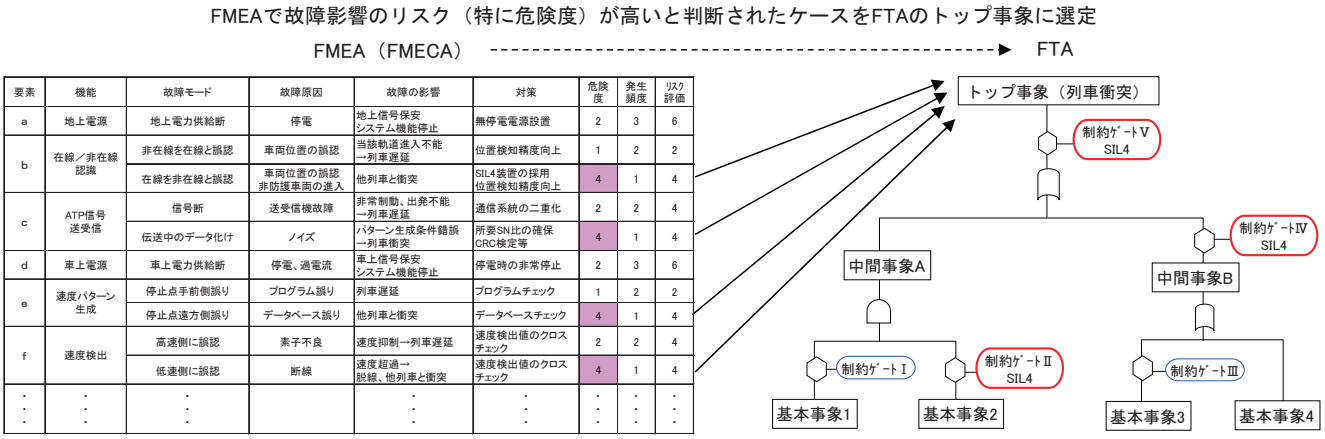
２．標準的な設計安全性評価手法の提示

２．１．FMEA と FTA の位置付け

これまでの当所の ISA 評価においては、FMEA と FTA を中核的な解析方法として活用している[2) 3)]。そこで示されている両者の関係を図１に示す。FMEA の拡張版である FMECA（Failure Mode and Effects Criteria Analysis）により、個々の要素の故障モード、故障要因、影響、対策等を検討し、影響度（危険性）、発生頻度、及びその両者で表されるリスク評価値を求める。そしてリスク評価値が大きいケース、その中でも頻度は小さいが危険性が高いケースを重点的に抽出し、FTA のトップ事象として選定する。FTA では、FMEA の結果に基づいて設定されたトップ事象からトップダウンで基本事象または非展開事象（以下「基本事象等」という）まで解析し、トップ事象に至る確率を算定する。さらに、基本事象等の中に FMEA で挙げた故障モード、対策等が漏れなく含まれていることを確認することにより FMEA の妥当性も検証する。また単一故障モードでは上位事象に至らないが複数故障モードの AND 条件により上位事象に至るような、FMEA では把握できない故障モードの影響も把握する。一方、安全性の可否の観点からは、基本事象等の発生確率に基づいてトップ事象の発生確率を計算するだけでなく、中間に介在する制約ゲートの機能の信頼性を確認することも有効である。そのため、制約ゲートの存在とその信頼性によりトップ事象の発生確率の小ささも評価する。

２．２．国際規格の考え方との整合

IEC 62425 では、FMEA は単一のフォールト（故障による異常状態）の影響解析、FTA は複数のフォールトの影響解析の主要な手段と位置付けられている[1)]。また、それらの手順や技法については IEC 60812 及び IEC 61025 に各々記述されている。



要素	機能	故障モード	故障原因	故障の影響	対策	危険度	発生頻度	リスク評価
a	地上電源	地上電力供給断	停電	地上信号保安システム機能停止	無停電電源設置	2	3	6
b	在線／非在線認識	非在線を在線と誤認	車両位置の誤認	当該軌道進入不能→列車遅延	位置検知精度向上	1	2	2
		在線を非在線と誤認	車両位置の誤認 非防護車両の進入	他列車と衝突	SIL4装置の採用 位置検知精度向上	4	1	4
c	ATP信号送受信	信号断	送受信機故障	非常制動、出発不能→列車遅延	通信系統の二重化	2	2	4
		伝送中のデータ化け	ノイズ	パターン生成条件錯誤→列車衝突	所要SN比の確保 CRC検定等	4	1	4
d	車上電源	車上電力供給断	停電、過電流	車上信号保安システム機能停止	停電時の非常停止	2	3	6
e	速度パターン生成	停止点手前側誤り	プログラム誤り	列車遅延	プログラムチェック	1	2	2
		停止点遠方側誤り	データベース誤り	他列車と衝突	データベースチェック	4	1	4
f	速度検出	高速側に誤認	素子不良	速度抑制→列車遅延	速度検出値のクロスチェック	2	2	4
		低速側に誤認	断線	速度超過→脱線、他列車と衝突	速度検出値のクロスチェック	4	1	4
・ ・ ・	・ ・ ・	・ ・ ・		・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

図１　FMEA（FMECA）と FTA の関係（模式図）[2)]

また状態遷移図を利用した確率計算の併用についても IEC 61025 に記述されている。そこで FMEA と FTA に関しては、これらの国際規格の記述を参照しながら、これまでの当所の手法を継承することとした。一方、IEC 62425、IEC 62278 等には安全性、ハザード、危害、重度、リスク等の一般的な用語に対しても明確な定義がなされており、また安全性を数値管理する SIL（Safety Integrity Level）や、安全性と信頼性等を一貫管理する RAMS（Reliability, Availability, Maintainability and Safety）の概念が記述されている。評価においては、これらの考え方との整合を図る。

２．３．標準的な設計安全性評価報告書の構成

これまでの当所における検討結果を踏まえて、標準的な安全性評価報告書の構成案を図2のような形で提案する。その主な内容は以下の通りである。

２．３．１．前段の項目

(1)評価対象範囲

ISA として責任を持つ対象範囲を明確に記述する。一方、ヒューマンエラー等、評価対象外の部分についても、国際規格の"Scope"（適用範囲）等を参考にして明示する。

(2)評価参照資料

評価の根拠とする参照資料として、評価依頼者から提示された各種の技術資料の全てに文書名、文書管理番号、日付が付与されたうえで報告書に明記する。

(3)参照する国際規格

評価において参照した主な国際規格を記載し、それらの国際規格と整合する評価であることを宣言する。

(4)システム概要

評価システムの全体像が、評価時点での当事者以外の関係者、また評価後の報告書閲覧者でも把握することを可能とするため、システムの概要を記述する。

２．３．２．安全性の評価結果

(1)システム構成及び個別要素の評価

システムの全体構成及び個別要素の各論的な評価結果を記述する。安全性が十分に高いと判断した根拠、更なる検討が必要とされた点、要注意な点、評価対象外ながら安全性への影響が大きい点等を述べる。

(2)FMEA による単一フォールトの影響解析

安全性への影響が予想される要素の故障モードを抽出し、各々の故障要因、影響、対策等を検討し、影響度（危険性の高さ）、発生頻度、及びその両者で表されるリスク評価値を求める。リスク評価値が許容限度を超える項目では低減対策を検討し再評価を行う。

(3)FTA による複合フォールトの影響解析

FTA では、FMEA でリスク評価値が大きいケース、特に頻度は小さいが危険度が大きいケースを抽出してトップ事象として選定する。基本事象等までの解析を行い、トップ事象発生を阻止する制約ゲートの存在とその信頼性を確認する。故障発生に時間差を含む事象等については状態遷移図等を別に作成して解析する。

(4)実機／実車試験

主にFTAの制約ゲートの機能を検証するため、実機、実車を用いた基本的な試験を行い、結果を記述する。

２．３．３．結言

安全性の評価結果をとりまとめた結論を記述し、また必要に応じて次の製造段階に向けた提言を行う。

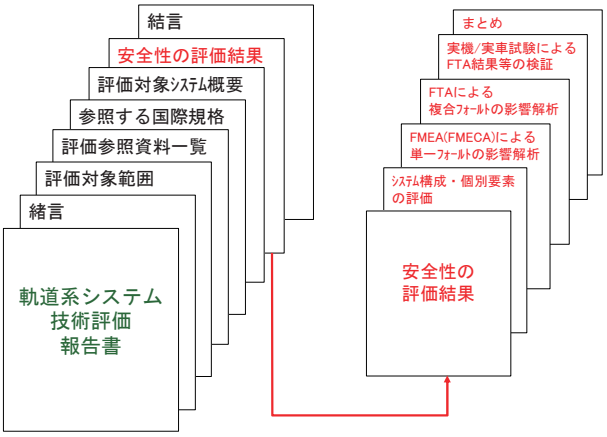


図２　標準的な設計安全性評価報告書の構成案

３．安全性と信頼性等について

３．１．RAMS の定義と相互関係

IEC 62278 によれば、RAMS（信頼性(R)、アベイラビリティ(A)、保全性(M)、安全性(S)）は表 1 及び図 3 のように示される[4)]。信頼性、保全性及び運用と保全の認識がアベイラビリティの技術的概念を形成し、それらのうち安全関連事項の認識が安全性の技術的な概念を形成するとされる[4)]。本報では主に安全性と信頼性の関係に注目し、安全性重視の方針を堅持しつつ、信頼性の向上も考慮した評価手法を検討する。

表１　RAMS の定義[4)]

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。

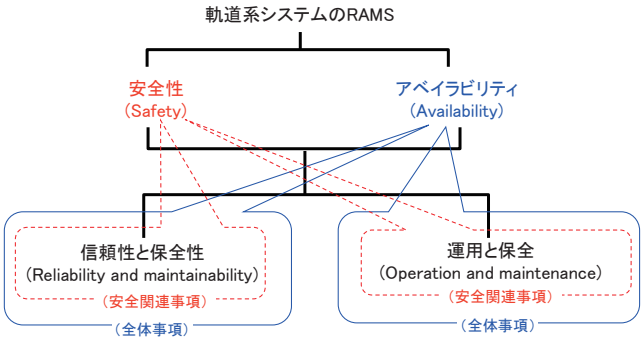


図３　鉄道の RAMS の相互関係 [4]

３．２．安全性と信頼性の関係

安全性と信頼性は必ずしも一致や包含関係を示すものではないとされ、両者の良否の組み合わせは表２のように示される [5]。①は本来の姿であり、②は安全性は確保されるが信頼性が低下するケース、③は信頼性は確保されるが安全性が低下するケースである。

表２　安全性／信頼性の良否の組み合わせ [5]

		信頼性	
		正常動作(○)	故障・停止(×)
安全性	安全(○)	①機器の動作が正常、かつ人に対して安全である状態	②機器は故障/停止しているが人に対しては安全である状態 (フェールセーフ)
	危険(×)	③機器は正常であるが使用時に危険になり得る状態	④機器が危険な状態で故障している (フェールアウト)

出典）門田「信頼性と安全性」、p. 13、表 1. 1. 1 日科技連出版社(2012)

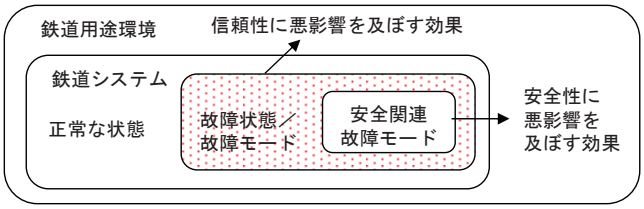


図４　システム内における故障の影響 [4]

表 2 の②④に相当する故障の影響に関しては、IEC 62278 によれば、図 4 のように整理される [4]。これについては前述のように FMEA、FTA 等で解析される。一方、③に関しては、故障を伴わないため FMEA では解析できず、評価対象外の要素やヒューマンエラーを含めて FTA により解析される部分であると考える。

３．３．日本の鉄道の現状

日本の鉄道等は、新幹線をはじめとして非常に高い安全性を有している。これは、故障検知による速やかな列車停止やフェールセーフが確立した信号システムの機能等によるものと考えられる。しかし一方で、近年は輸送障害が増加傾向を示し、大都市圏では運休や遅延が拡大して、信頼性（稼働率等）がやや低下しているといえる。障害には設備や車両の故障に起因する事例が少なくなく、特に障害発生時には全線で運転を停止し、復旧後に一斉に運転を再開するような手順が採られる都市部の鉄道路線においては長時間にわたり広域的な輸送影響を及ぼすこととなる [6]。したがって、故障の復旧時間を短縮することが、信頼性を含むアベイラビリティの向上に寄与するものと考える。

４．故障予知を活用した新たな FMEA の提案

４．１．従来の FMEA

従来の FMEA（または FMECA）では、故障の影響度の評価として、故障検知後に停止させる等の適切な対策を採って許容レベル以下にする手法が用いられている。許容リスクを評価する方法としては、RPN(Risk Priority Number)を用いることがある。これは、RPN=故障ﾓｰﾄﾞ発生頻度(λ)×影響度(ε)×検出度(β)と定義して、発生頻度、影響度を点数化し、RPN の値により発生するリスクが許容可能かを判断するものであり、IEC 62278 の考え方にも記されている [4] [6]。RPN による許容リスク評価例を表 3 に示す [6]。

表３　影響度と発生頻度による許容リスク評価例 [6]

			影響度			
			Insignificant	Marginal	Critical	Catastrophic
			1.0	2.0	3.0	4.0
発生頻度	Frequent	6.0	6	12	18	24
	Probable	5.0	5	10	15	20
	Occasional	4.0	4	8	12	16
	Remote	3.0	3	6	9	12
	Improbable	2.0	2	4	6	8
	Incredible	1.0	1	2	3	4

RPN= 発生頻度×影響度×検出度 （検出度=1と仮定）	12＜RPN	8＜RPN≦12	4＜RPN≦8	RPN≦4
	Intolerable	Undesirable	Tolerable	Negligible

ここでは検出度を 1 と仮定して、RPN=λ×ε として数値化し、リスクを Negligible、Tolerable、Undesirable、Intolerable に分け、Negligible 、Tolerable を許容可能なレベル（本報では点数 8 点以下）としている。発生頻度（故障率）、影響度を表 3 のように点数化して RPN を求めた駅ホームのホームドアの扉駆動モータに関する FMEA の例を表 4 に示す。故障モード「絶縁不良」を例とすると、頻度=3、影響度=3 で RPN=9 となり、許容不可となる。

４．２．信頼性の指標

信頼性の指標としては、故障率（λ）、稼働率（A）等が挙げられる。故障率は平均故障間隔 MTBF（Mean Time Between Failure）の逆数として表される。

$\lambda = 1/(MTBF)$ (/h) (1)

また、稼働率は、MTBF と平均修復時間 MTTR (Mean Time to Repair) から、

$A = MTBF/(MTBF + MTTR)$ (/h) (2)

で表される。修復率を μ (=1/MTTR) と定義すると、

$A = \mu/(\lambda + \mu)$ (/h) (3)

となる。したがって、稼働率を上げるには、故障率を下げるか修復率を上げれば良いことがわかる[6]。

4．3．故障予知を考慮した FMEA (FMEPA)

この従来の FMEA に対して、故障予知の概念を入れた評価を試みた[6]。その一環として、FMEA の中に故障予知の因子、指標、精度を追加して、故障の影響解析を行う手法を FMEPA (Failure Mode, Effects and Protect Analysis) として提案する。表 4 の FMEA 実施の例を基にした、FMEPA による解析例を表 5 に示す。FMEPA では、故障モードと推定原因の次に、故障予知可能な因子を抽出し、予知のための検出方法を示すとともに、予知精度を評価する。予知が成功すれば、故障前の処置によって修復時間を最小化し稼働率の低下を防止することができる。例えば、動作電流の変化により「断線」が予知できれば、故障前の部品交換によりシステム停止時間を最小限に留めることが可能となる。また過熱に対しては、上限温度に達する前に電流制限等を行って動作を継続させれば、稼働率の向上につながる。ここで各故障モードの頻度 (故障率) を λ_i、予知の成功確率 (以下「予知率」という) を α_i、予知率を考慮した頻度を λp_i (i=1～4) とすると、

$\lambda p_i = (1-\alpha_i) \times \lambda_i$ (ただし $0 \leqq \alpha_i \leqq 1$) (4)

と表される。「絶縁不良」(i=2) における、予知の定量的な効果をみると、頻度は従来の 3 から $3\times(1-\alpha_2)$ に減少する。この故障モードの影響度は3であるから、

$RPN=3\times(3\times(1-\alpha_2))$ (5)

となり、$\alpha_2 \geqq 1/9$ であれば、$RPN \leqq 8$ となるため、新たな故障対策を採らなくても 4.1 で前述した許容リスク内に収まることとなる。

5．まとめ

これまでの当所での検討に基づいた、国際規格と整合する標準的な安全性評価報告書の構成案を提案した。また安全性重視を堅持しつつ信頼性等も考慮した技術評価手法に検討の第 1 歩として、従来の FMEA に故障予知を考慮した FMEPA によるリスク評価を試みた。今後はアベイラビリティ、保全性を含めた RAMS の一貫した技術評価手法の構築に向けた取り組みを続けていく。

参考文献

1) IEC 62425 Edition 1.0 2007-09

2) 水間「安全技術のチェンジ」電気学会産業応用部門大会前刷集Ⅲ、pp. 143～146 (2009)

3) 林田等、交通安全環境研究所ﾌｫｰﾗﾑ 2014 講演概要

4) IEC 62278 First edition 2002-09 英和対訳版

5) 門田「信頼性と安全性」、pp. 12-14、日科技連出版社(2012)

6) 水間他「故障検知・予知を考慮した鉄道の信頼性解析手法の検討」日本信頼性学会「信頼性」論文(投稿中)

表 4　従来の FMEA (FMECA) による RPN の算定

アイテム	機能	故障モード	推定原因	故障の影響		頻度	影響度	RPN
				サブシステム	システム			
扉駆動モータ	扉を開閉する	断線	劣化	扉が動かない	乗降ができない	2	2	4
		絶縁不良	劣化	漏電	感電	3	3	9
		過熱	過負荷	扉が動かない	乗降ができない	4	2	8
		暴走	フェールアウト故障	異常開閉	転落等	1	5	5
		・ ・	・ ・	・ ・	・ ・	・ ・	・ ・	・ ・

表 5　故障予知を考慮した FMEPA による RPN の算定 (各故障モードの推定原因等は表 4 と同じ)

アイテム	機能	故障モード	従来のFMEAによる評価			故障予知を考慮した評価				
			頻度	影響度	PRN	故障予知因子	故障予知の検出方法	故障の予知率	予知率を考慮した頻度	予知率を考慮したRPN
扉駆動モータ	扉を開閉する	断線	2	2	4	電流変化	動作電流変化	α_1	$2\times(1-\alpha_1)$	$4\times(1-\alpha_1)$
		絶縁不良	3	3	9	電流変化	絶縁抵抗変化	α_2	$3\times(1-\alpha_2)$	$9\times(1-\alpha_2)$
		過熱	4	2	8	モータ温度上昇	温度変化	α_3	$4\times(1-\alpha_3)$	$8\times(1-\alpha_3)$
		暴走	1	5	5	無し	無し	α_4 (=0)	$1\times(1-\alpha_4)$ (= 1)	$5\times(1-\alpha_4)$ (= 5)
		・ ・	・ ・	・ ・	・ ・	・ ・	・ ・	・ ・	・ ・	・ ・