

⑧ 海外展開を踏まえた軌道系交通システムの 安全性評価手法に関する検討

交通システム研究領域

※林田 守正

廣瀬 道雄

大野 寛之

森久 至

森 裕貴

1. はじめに

海外展開を視野に入れた鉄道等の軌道系交通システムの安全性については、リスク数値管理やRAMS（後述）等の概念を含んだ国際規格とも整合する客観的な第三者評価が求められている。本報告では、交通安全環境研究所（以下「当研究所」という）が実施している安全性評価事例をモデルケースとした、国際的にも受容される標準的な評価手法の提示に向けた検討状況について述べる。なお、本報告では第三者安全性評価者をISA（Independent Safety Assessor）、ISAによる安全性評価をISA評価と表すこととする。

2. 安全性評価手法標準化の検討対象とモデル

当所では様々な軌道系交通システムに関するISA評価を行っており、そのうち図1に示すような、索道関係等を除く事例の設計安全性を本検討の対象と位置づけている。過半を占める信号保安システムの場合は制御出力までが評価範囲であるが、近年行っている新方式ホームドアやブレーキシシステム等では、動作部分も含めたシステム全体が評価対象となる。

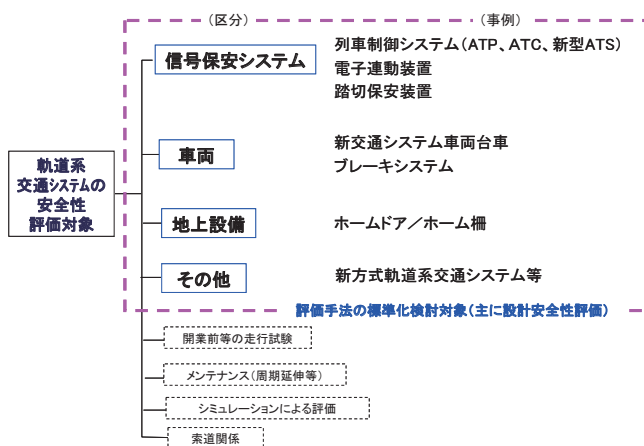


図1 安全性評価手法の標準化検討の対象

また評価事例の約3/4が海外展開を意識したものである一方、国内のニーズに基づいて開発され、先ずは

国内での実用化を図る事例もある。特に後者の事例では将来的な海外展開に向けての課題が多いと考えられる。当所では、これらのISA評価事例をモデルとして安全性評価手法の標準化に関する検討を行った。

3. 評価手法の国際規格との整合

3. 1. 整合／参考の対象とする国際規格

鉄道に関する主要な国際規格としては、表1に示すようなIEC（国際電気標準会議）規格や、ISO（国際標準化機構）規格が挙げられる。そのうち、まずISA評価手法として国際的に必要とされる可能性が高いIEC 62425（信号保安用電子機器のセーフティケース）およびIEC 62278（RAMS）の2規格との整合について、検討することとした⁽¹⁾⁽²⁾。ただしそれ以外の規格も参照し、特に都市鉄道の評価については、検討継続中ではあるが、IEC 62267やIEC 62290に記述される用語、定義等も参照することとした。

表1 整合／参考の対象とする国際規格の例⁽¹⁾⁽²⁾

規格番号	規格の題目
IEC61508-1～7	安全に関連する電気/電子/プログラマブル電子装置（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
IEC62267	AUGT 無人運転の安全性要件
IEC62290	UGTMS 輸送システムの管理と指令
IEC 62247	車両と列車検知システムの共存性

3. 2. 国際規格の主要な概念の整理

3. 2. 1. IEC 62425におけるISA評価の要求

軌道系システムの海外展開事例では、導入先の事業者側からISA評価が必要とされるケースが増加している。その根拠として、例えばIEC 62425では、メーカー等が作成するセーフティケース等に加え、ISA評価（および報告書）が必須であるとしている⁽¹⁾。その位置付

けを図2に示す。IEC 62425に規定されるISA評価範囲は、品質や安全のマネジメント体制にも及ぶ広汎なもの（広義のISA評価）である。これに対し、本報告における安全性評価手法標準化の検討範囲は、当所がこれまで主に行ってきた、Technical safety reportに該当する安全関連の技術評価（狭義のISA評価）に限定する。そしてISAとしての評価の実施や報告書の作成に際しては、IEC 62425等における規定を十分に理解して認識し、可能な限り整合を図っていく必要がある。

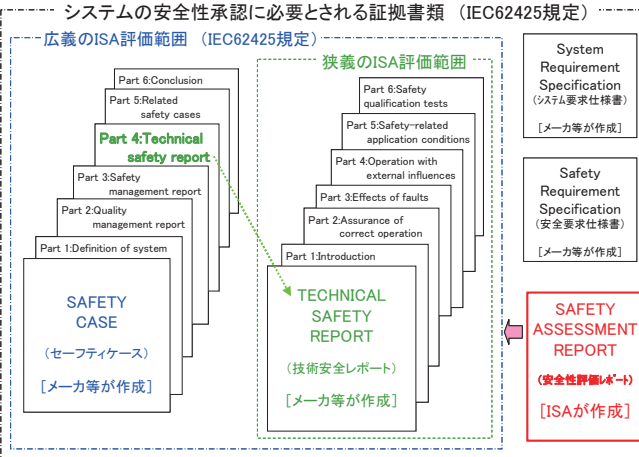


図2 IEC 62425に規定されるISA評価の位置付け⁽¹⁾

3. 2. 2. RAMSの相互関係

IEC 62278においてはRAMSの構成要素として、安全性 (Safety) と共に信頼性 (Reliability)、アベイラビリティ (Availability)、保全性 (Maintainability) について記述されている。またRAMSの管理プロセスが規定され、IEC 62425でも参照されている。RAMSの各要素の相互関係は図3のように示されている。

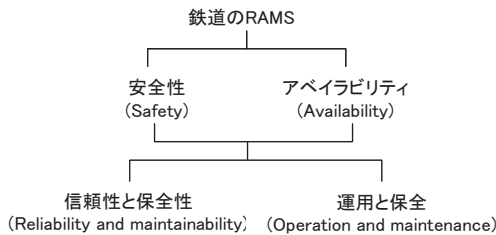


図3 鉄道におけるRAMSの相互関係⁽²⁾

特に安全性はアベイラビリティの影響要因の一部（安全性関連）を共有し、密接な関連を有するとされる⁽²⁾。またアベイラビリティの低下は安全性低下の遠因になることも予想される。したがって評価に当たっては、単に安全か否かの判断だけでなく、アベイラビリティとの両立や相反にも考慮する必要がある。

3. 3. 具体的な検討例

3. 3. 1. 評価対象範囲の明確化

評価対象範囲は、ISA評価の大前提となる事項である。ISAとして責任を持つ対象範囲を明確にし、併せて、ヒューマンエラー等、ISA評価の対象外の部分については、国際規格における“Scope”等の記述を参考にして明示することにより、評価対象範囲に関して依頼側と齟齬を来さないよう留意する必要がある。

3. 3. 2. 参照資料の明記

ISA評価では評価の根拠となる参照資料として、評価対象システムに関する各種の技術資料が提示される。ISA評価完了後の資料特定や履歴管理を可能とするため、全ての参照資料には各々文書名、文書管理番号、日付が付与されることがし、報告書に明記して、各文書との関連がわかるようにする必要がある。

3. 3. 3. 用語、略語の定義

安全、エラー等の、一般的な安全性関連用語の意味は自明と扱われがちであるが、実態は曖昧であったり、海外とは認識が異なったりするケースが多い。一方IEC 62425等の国際規格では表2に例示するように、用語、略語の意味が具体的に定義されている⁽¹⁾⁽²⁾。

表2 安全関係の主要用語の定義（例）⁽¹⁾⁽²⁾

用語	IEC62425 (セーフティケース)		IEC62278 (RAMS)	
	英文	和文	英文	和訳
safety		安全	freedom from unacceptable levels of risk of harm	許容できない危害が発生するリスクが無いこと。
risk		危険度 リスク	the combination of the frequency, or probability, and the consequence of a specified hazardous event	ハザードの発生確率及び発生する危害の重大度。
error		誤り エラー	a deviation from the intended design which could result in unintended system behaviour or failure	—
failure		故障	a deviation from the specified performance of a system	—
fault		欠陥	an abnormal condition that could lead to an error in system NOTE a fault can be random or systematic	—
hazard		潜在危険 ハザード	a condition that could lead to an accident	Physical situation with a potential for human injury and/or damage to environment 人的傷害及び／又は環境ダメージを起こし得る物理的状況。
reliability		信頼性 信頼度	the ability of an item to perform a required function under given conditions for a given period of time	probability that an item can perform a required function under given conditions for a given time interval (t1,t2) 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

したがって国際規格における安全性関連の主要用語の定義を原文（英語等）で把握し、報告書にも明示すると共に、評価文中で適確に使用して、評価結果の解釈に齟齬をきたさないよう注意する。また評価対象システム特有の用語、略語の定義についても確認のうえ、報告書に明記する。

3. 4. FMEA および FTA について

3. 4. 1. 当所の FMEA/FTA の方針と特徴

当所の ISA 評価では FMEA（または FMECA）と FTA を中核的な手法として用いており、特に重大な危険事象の発生頻度は十分に低いことを確認するよう留意している⁽³⁾。従来は、その評価基準を、日本の鉄道の安全性と同程度以上としていたが、近年は国際規格を意識して数値化（例えば $10^{-9}/h$ 以下）している。また FMEA の結果を踏まえて FTA のトップ事象を決定し、さらに両者の結果の整合性を確認している⁽³⁾。なお安全性評価においては、トップ事象に至る確率が十分に小さいことを明確にすれば十分であるため、主に制約ゲートの存在とその信頼性（SIL(Safety Integrity Level)等）を明確にすることが効率的であると考ええる。さらに、制約ゲートの確からしさを実車試験等により検証している。また FTA では把握しきれない、動的な事象解明には、状態遷移図を利用した確率計算も併用している。

3. 4. 2. FMEA/FTA の例（昇降式ホームドア）

乗降客が多い駅では、ホームからの転落や接触事故の防止のため、ホームドアが普及しつつあるが、ドア数が異なる車両への対応やコスト低減のため、軽量構造の昇降式ホームドアが新たに開発された。その試作例を図 4 に、一般化した想定機能を表 3 にそれぞれ示す⁽⁴⁾。FMEA、FTA の一例として、昇降式ホームドアをモデルケースとした解析について記述する。まず、昇降式ホームドア特有の構成部品について、その故障モードと影響解析を FMEA として行うこととする。



図 4 昇降式ホームドアの試作例（左：ロープ式 右：バー式）

表 3 昇降式ホームドアの想定機能

項 目	昇降式ホームドア	左右開閉式ホームドア(従来型)
スクリーンの開閉方向	上下方向	水平方向
スクリーンの構成	水平に並行する複数のロープ、バー等	板状のドア
スクリーンの動き	支柱に支持・案内されロープ/バーの間隔や重なりを変えながら昇降	戸袋に支持・案内され左右にスライド
支持案内支柱の伸縮	機種によって有り	無し
動力源	モータ	モータ
人・物体の近接検知	有り	無し
ドア挟み込み検知	有り	有り
線路側取り残し検知	有り	有り
スクリーン開閉操作	列車到着／出発検知と連動した自動開閉または乗務員等による手動操作(切替)	列車到着検知等と連動した自動開閉または乗務員等による手動操作(切替)
開閉制御モード(1)	一斉または個別(切替)	一斉または個別(切替)
開閉制御モード(2)	自動または手動(切替)	自動または手動(切替)
停車直前／発車直後の開閉	機種によって有り(自動モード)	無し(開閉は停車中に限定)

表 4 に、このような考え方に基づいて行った FMEA の例を示す。電源断、モータ故障、部材破損、操作盤スイッチ故障がスクリーンの落下／降下を引き起こし、センサ類の故障が荷物や人を巻き込んだスクリーンの上昇に繋がること等が予測できる。表 4 の FMEA の結果を考慮すると、昇降式ホームドアに特有な危険事象（ハザード）の例として、以下のような事象が予測される。

- ・ 降下するスクリーンが旅客に接触または衝突
- ・ 荷物立掛け、旅客もたれ掛けりの状態でスクリーン上昇
- ・ 通過列車を停車と誤認してスクリーン上昇

表 4 昇降式ホームドアに関する FMEA の例（一部）

No	ブロック	故障モード	故障発生タイミング	故障の影響	想定されるハザード	対策	危険度	発生頻度	リスク評価
1	モータ電源	電源供給断	閉状態以外	スクリーンが不意に降下する	上方から旅客に衝突	位置保持機構または無停電電源を備える	4	2	8
2	モータシステム	モータ本体または制御機器の故障により軸トルクが喪失	開状態	スクリーンが不意に降下する	上方から旅客に衝突	実績がある製品を使用 位置保持機構を備える 一定時間内に完了しない場合は警報出力(降下が正常時より遅くなる場合)	8	1	8
3			閉状態	開動作できない	車両ドア開の遅れ		1	2	2
4			開動作中	開動作が停止し降下に転じる	上方から旅客に衝突		4	1	4
5			開動作中	重力により降下する(正常時より速くなるか遅くなる)	上方から旅客に衝突、又は旅客の転落、触車		8	1	8
6	昇降機構	ロープ／バー／支柱昇降用ワイヤの破断	閉状態以外	スクリーン／支柱の全体又は一部が落下する	上方から旅客に衝突	十分な強度設計および点検整備	4	1	4
7		ロープ／バー／支柱昇降用釣合機構の破損	閉状態以外	破断したロープ／バーが落下、飛散する	旅客に当たる		4	1	4
8	スクリーン構成	ロープ／バーの破断	全状態	破断したロープ／バーが落下、飛散する	旅客に当たる	十分な強度設計および点検整備	4	1	4
9		ロープ／バーのホルダーからの外れ	全状態	外れたロープ／バーが落下、飛散する	旅客に当たる		4	1	4
10	操作盤(一斉／個別)	開閉スイッチ故障(誤って閉指令)	開状態	乗降中にスクリーンが降下する	上方から旅客に衝突	実績がある製品を使用 ノイズ対策	2	2	4
11		開閉スイッチ故障(誤って開指令)	閉状態	列車が到着していないのにスクリーンが上昇する	旅客の転落、触車		8	1	8
12		モード切替スイッチ故障(誤って手動モード)	開状態	発車後も開動作しない	旅客の転落、触車		8	1	8
13		列車が到着したのに到着していないと誤検知(センサ正面の障害物等による検知妨害)	閉状態	ドアが開かない(自動開閉モードの場合)	車両ドア開の遅れ		1	3	3
14	列車到着／出発検知センサ	ケーブルのコネクタ外れ	閉状態	ドアが開かない(自動開閉モードの場合)	車両ドア開の遅れ	コネクタ外れの検知 鳥等による誤検知の防止検討 実績がある製品を使用 ノイズ対策	1	2	2
15		列車が到着していないのに到着したと誤検知	閉状態	スクリーンが上昇する(自動開閉モードの場合)	旅客の転落、触車		8	1	8
16		列車が発車していないのに発車したと誤検知	開状態	スクリーンが降下する(自動開閉モードの場合)	上方から旅客に接触		2	2	4
17		近接物が無いのに近接物有りと判断	開動作中	開動作が中断する	車両ドア開の遅れ		1	2	2
18	近接物検知センサ	近接物が有るのに近接物無しと判断	閉動作中	閉動作が中断する	旅客の転落、触車	実績がある製品を使用 ノイズ対策 自己診断機能により検出	8	1	8
19		近接物が有るのに近接物無しと判断	閉状態	人が近付いても警告されない	旅客や荷物を引っ掛け たまま上昇		2	2	4
20			開動作中	人が近付いても警告されない			2	2	4
21			開動作中	人が直下に来てでも開動作を停止しない	上方から旅客に接触		2	2	4

(危険度:1,2,3,8 発生頻度:1,2,3 許容リスク:8以下)

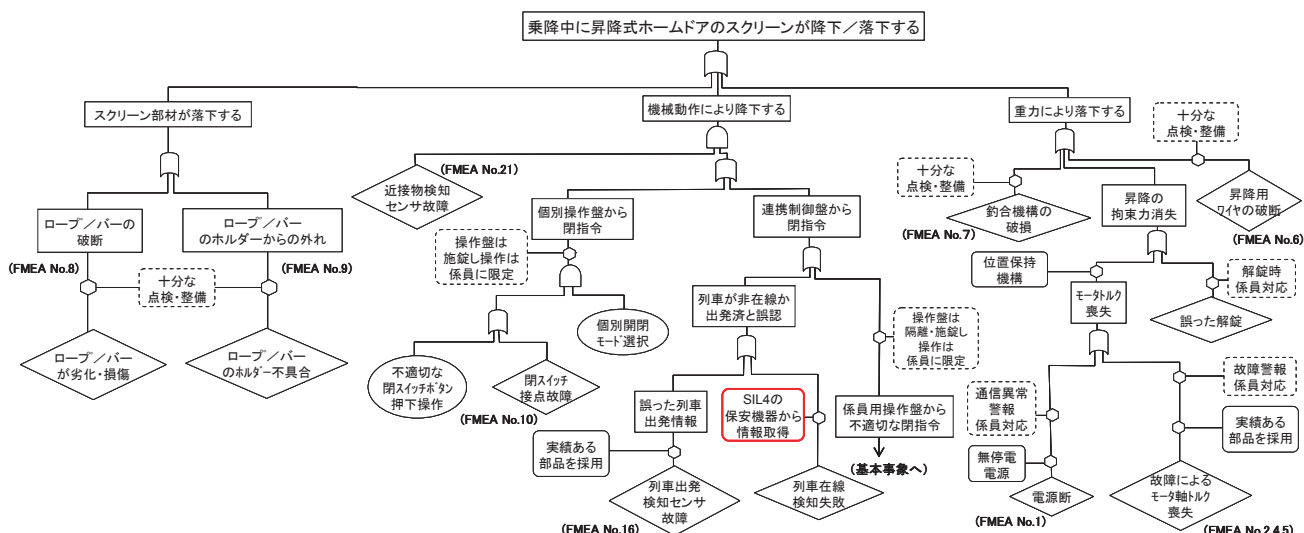


図5 昇降式ホームドアに関する FTA の例（一部）

図5に、上記の FMEA の結果とハザード予測に基づいた FTA の一例を示す。トップ事象の一つとして、昇降式特有の危険事象である、乗降中にスクリーンが不意に落下／降下して旅客に接触または衝突する事象を設定し、中間事象を経て、基本事象とそれらの発生確率までを解析する。制約ゲートにはシステムによる防護と運用による防止があり、前者は故障確率の同定、後者は事業者側との協議によるルール化が重要である。またホームドアの開閉動作が正常でも旅客の不適切な行動によって生じるハザードも存在するため、例えば旅客の故意による危険行動に対しては防護の対象外とする等の整理が必要である。

3. 4. 3. FMEA/FTA の国際規格との整合

IEC 62425 では、Technical Safety Report の“Effects of faults”において FMEA と FTA の活用が推奨され、前者は単一欠陥の検出、後者は複合欠陥の影響の解析手段として挙げられている⁽¹⁾。また FMEA、FTA の手順の主要段階や技法は IEC 60812、IEC 61025 に記述され、状態遷移図を利用した確率計算の併用についても IEC 61025 において記述されている⁽⁵⁾⁽⁶⁾。そこで FMEA、FTA に関しては、これらの国際規格の記述を考慮しながら、これまでの手法を継承する。国際規格の FMEA、FTA に関する記述は概ね緩やかな指針であるため、整合は比較的容易であると考えるが、FMEA におけるリスクの定量評価や FTA における制約ゲートの表現方法等については検討を加える必要がある。

3. 5. 標準的な安全性評価報告書の構成

以上の検討結果に基づいて、表5のような ISA としての安全性評価報告書の構成の一例を考えた。各部の

詳細については今後検討を続け、最終的にはマニュアル化に繋げていく予定である。

表5 安全性評価報告書の基本構成例

番号	項目
1	序文
2	評価対象範囲
3	参照資料リスト
4	用語、略語の定義
5	参照する国際規格
6	評価対象システムの概要
7	技術的な要点的抽出と評価
8	FMEAによる単一フォールトの影響解析
9	FTAによる複合フォールトの影響解析
10	実機・実車試験によるFTA等の検証
11	結論

4. まとめ

当所の ISA としての安全性評価事例をモデルケースとして、整合、参照すべき国際規格と主な概念を念頭においた標準化への具体的な取組みを整理した。また当所がこれまで中核的に用いてきた FMEA、FTA の手法の特徴と事例について述べ、国際規格との整合性と、安全性評価報告書の構成に関する方向性を示した。

参考文献

- (1) IEC 62425 Edition 1.0 2007-09
- (2) IEC 62278 First edition 2002-09 英和对訳版
- (3) 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 pp.143～146 (2009)
- (4) 森「ホームにおける安全・安心向上への取組み」平成 26 年度交通安全環境研究所講演会講演概要
- (5) IEC 60812 Second edition 2006-01 英和对訳版
- (6) IEC 61025 Edition 2.0 2006-12