# ⑩ RAMS の概念に基づいた軌道系交通システムの総合的な技術評価について

交通システム研究部　※林田 守正　廣瀬 道雄　大野 寛之　緒方 正剛　竹内 俊裕　工藤 希
理事　水間 毅

## 1．はじめに

軌道系交通システムの長期運用に関わる評価法として、国際規格 IEC 62278 で信頼性(R)、アベイラビリティ(A)、保全性(M)を安全性(S)と共に評価対象とする RAMS の概念が定義され [1]、国内外で総合的な技術評価の指標と考えられるようになった [2]。これまで第三者の立場で数多くの安全性評価を行ってきた当所でも、信頼性等の観点を含む総合的な評価手法の構築をめざしている。本報告では従来の当所の安全性評価や国際規格における技術評価の考え方を整理した上で、実際の評価事例から安全性と信頼性の観点の相違を抽出する一方、近年普及が進んでいる信頼性解析専用ソフトウェアの活用に関する検討状況について述べる。

## 2．総合的な技術評価に向けた考え方の整理

### 2．1．これまでの安全性評価の観点

わが国の鉄道の安全性は世界的にも最高水準といえる。これは様々な安全性技術により信号システム等のフェールセーフを実現している結果といえる [2]。当所の第三者安全性評価においても、国際規格の SIL (Safety Integrity Level) 等の概念を採用しつつ、安全性の担保を最重視する方針を堅持してきた。一方、危険防止のための予防保全（システム停止等）や、安全側の故障については、副次的に扱ってきた点は否めない。

### 2．2．国際規格の安全性と RAMS に関する考え方

IEC 62278 等の国際規格では「絶対安全は存在しない」という考え方に基づき、安全について、リスク（危害の発生確率と危害の重度の組み合わせ）の概念を経て、「受入れ不可能なリスクが無いこと」と定義している [3]。またリスク受入れの原則として ALARP (As low as Reasonably Practicable：現実的に実現可能な限り低いこと）等の考え方が示されている。このような安全性に関する考え方は、これまで「絶対安全」の考え方に基づいてきたわが国には馴染みにくいが [3]、鉄道技術の国際展開には考慮が不可欠と考えられる。

安全性だけでなくアベイラビリティ等を含めた総合的な評価要素として、RAMS が表 1 のように定義されている [1]。本報告では安全性と、アベイラビリティ形成の主な要素である信頼性の関係に注目して、当所の安全性評価事例から抽出した、安全性と信頼性の観点が相違するケースを 3 章に後述する。

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。 |

## 3．評価事例にみる安全性と信頼性の観点の相違

### 3．1．無線式列車制御システムの通信異常

近年、鉄道信号は従来の軌道回路による列車検知を用いたシステムに代わり、図 1 に示すような無線式列車制御システム（CBTC：Communication Based Train Control）の開発、普及が進んでいる。

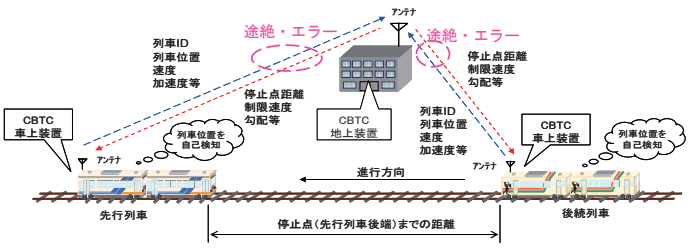


図 1　無線式列車制御装置（CBTC）の概要

CBTC では列車上で検知した位置を地上装置に無線送信することにより在線情報を管理するため、途絶、データエラー等の通信異常が発生した場合は列車位置不明となる。その観点は以下の通りとなる。

①安全性の観点：通信途絶時間、パケットエラー率等が所定の閾値を超えた場合、設計通り確実に非常ブレーキが作動すれば問題無し。

②信頼性の観点：通信途絶、通信エラー等により列車運行が停止する頻度が高すぎれば問題有り。

本評価事例では、通信途絶許容時間の妥当性について検討を重ね、実車試験による検証を行った。

### 3．2．制御論理部のフェールセーフと冗長性

信号保安装置等の制御論理部はフェールセーフ設計が採用されるが、評価の観点は以下の通りとなる。
①安全性の観点：錯誤動作につながるような危険側故障率が閾値以下（例えばSIL4）であれば問題無し。
②信頼性の観点：安全側/危険側故障に関わらず、誤って停止信号となる頻度が高すぎれば問題有り。

本評価事例では、危険側/安全側故障率を把握すると共に、信頼性や稼働率についても言及する。

## 4．信頼性解析専用ソフトウェアの活用

### 4．1．信頼性解析専用ソフトウェアの概要

当所ではこれまでFMEA（Failure Mode and Effects Analysis）やFTA（Fault Tree Analysis）による安全性、信頼性の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りのツールを利用する手法（以下「従来手法」という）を用いてきた。一方、近年は既成の信頼性解析専用ソフトウェアを活用する手法（以下「専用ソフト手法」という）も普及している。専用ソフトの一例について個別機能と相互関連を図2に、FMEAの試行例を図3にそれぞれ示す。

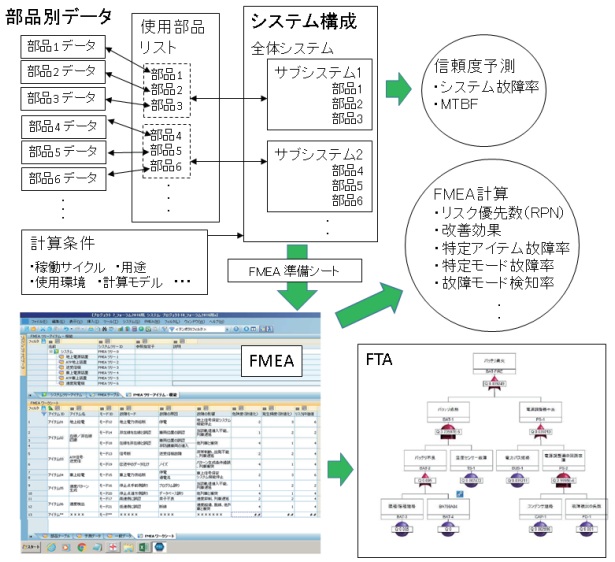


図2　専用ソフトウェアの個別機能と相互関連（例）

### 4．2．従来手法と専用ソフト手法の比較

専用ソフト手法の、個別部品データからシステム構成を定め、FMEA、FTAに進む過程は従来手法と同様である。従来手法の特徴である、FMEAの結果に基づいてFTAのトップ事象を選定する点は踏襲可能である。専用ソフト手法の特徴としては以下の点が挙げられる。

(1)個別部品データからFMEA、FTA等に至る手順を定型化し、個人差による結果の差異を縮小する。
(2)大量の部品データ等をデータベース化し、検索/入力作業の効率化や洩れの防止を図る。
(3)解析を階層構造（プロジェクト＞システム＞FMEA・FTA）とし、プロジェクト又はシステム単位で計算式、部品データ、使用部品リスト、システム構成等を設定/共有して、システム毎に複数のFMEA、FTAを行う。
(4)同一システム内の部品データ、使用部品リスト、システム構成を相互に関連付けして整合性を保ち、IEC 62278等で重視されるトレーサビリティを確保する。

上記のうち(1)(2)は従来手法の支援機能であると考えるが、(3)(4)は専用ソフト手法特有のアプローチであるといえる。このことを利用して、信頼性、稼働率の定量化を図り、従来の安全性に関する定量化とのバランスを考慮した評価が可能になると考える。また、今後はFTAやマルコフ解析等も含め、従来手法と専用ソフト手法の比較を深度化し、総合的な技術評価の確立に向けて、それらの得失について検討、整理を進めていく予定である。

図3　専用ソフト手法によるFMEAの試行例（一部）

## 5．まとめ

(1)国際規格の安全性やRAMSの考え方を整理し、評価事例から安全性/信頼性の観点の相違を抽出した。
(2)信頼性解析専用ソフトウェアを活用した信頼性、安全性の評価手法について検討した。

## 参考文献

1) IEC 62278 First edition 2002-09 英和対訳版
2) 平栗，″信号システムの安全性″，第22回鉄道総研講演会予稿集 p. 43-52（2009）
3) 向殿，″日本と欧米の安全・リスクの基本的な考え方について″，標準化と品質管理，p. 4-8，（2008）