⑧鉄道システムの第三者安全性評価と国際規格 IEC 62425 の接点について

交通システム研究部　　※林田 守正　　工藤 希
鉄道認証室　　森 崇

1．はじめに

当研究所では、各種の鉄道に関する第三者安全性評価（以下「安全性評価」）を行ってきた[1]。しかし近年、日本の鉄道システムの輸出に際しては、IEC (International Electrotechnical Commission) シリーズ等の国際規格への適合が求められるようになっている。本報告では、主に信号システムのハードウェアに関する安全性評価と、それに関連が深いと考えられる IEC 62425 との接点に着目し、FTA (Fault Tree Analysis) 等のリスク解析を例として、フェールセーフ性の考え方やその担保の技法について考察した結果を報告する。

2．安全性評価と IEC 62425 の項目

当研究所の安全性評価報告書の項目例と、IEC 62425 に規定される Safety Case の項目との対応を図 1 に示す[2]。安全性評価報告書の「安全性評価結果」の各項目と主に関連するのは、Safety Case Part 4: Technical Safety Report の各 Section であると考える。また IEC 62425 Annex A～E には安全インテグリティ（Safety Integrity）の考え方、安全性を担保するための技術と対策等が記述されているため、これらも安全性評価結果の各項目と対応すると考える。一方、IEC 62425 5.5 Safety acceptance and approval では、システムの安全性の承認に際して、Safety Case 等の他に、第三者安全性評価が必要であるとされている[2]。当研究所の安全性評価では FMEA（FMECA 及び FMEDA を含む）及び FTA によるリスク解析を中核としているため[1]、本報告では特にそれらと関連が深いと考える Technical Safety Report の Section 2: Assurance of correct operation 及び Section 3: Effects of faults、並びに Annex B 及び Annex E の記述との対応について重点的に考察した。

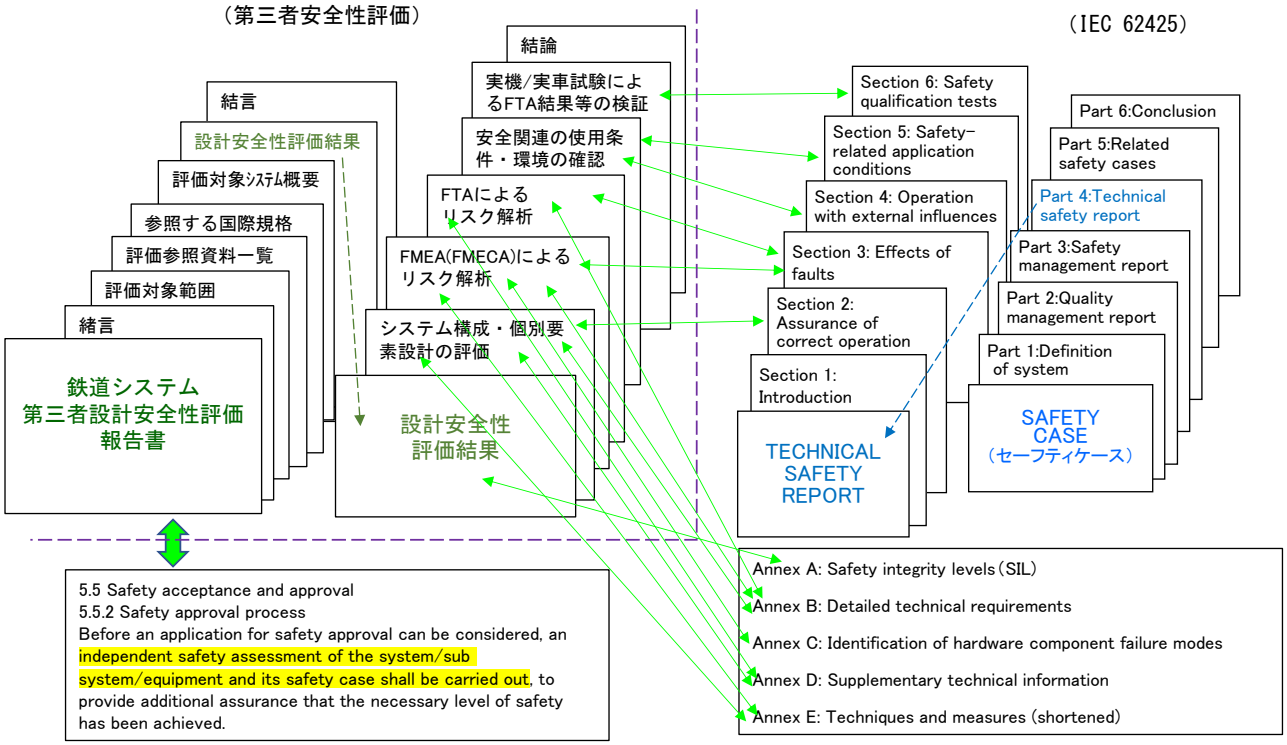

図 1　安全性評価報告書の項目例と IEC 62425 の構成[2]

３．対応例の検討例

３．１．システム要求と安全関連要求

IEC 62425 に記述される、システム要求仕様における安全インテグリティ要求の位置付け、及び安全性評価との対応を図 2 に示す[2]。安全インテグリティは系統的（システマティック）故障に対するものと偶発的（ランダム）故障に対するものに二分され、前者は定性的な安全性評価、後者は定量的な安全性評価に対応すると考える。安全インテグリティのレベル（SIL: Safety Integrity Level)は 3.2 に後述するように 4 段階が定義される。安全性評価は指定された数値目標をクリアし、既存の類似システムと同等以上の安全性の確保の達成を判断基準とする事例が多い。

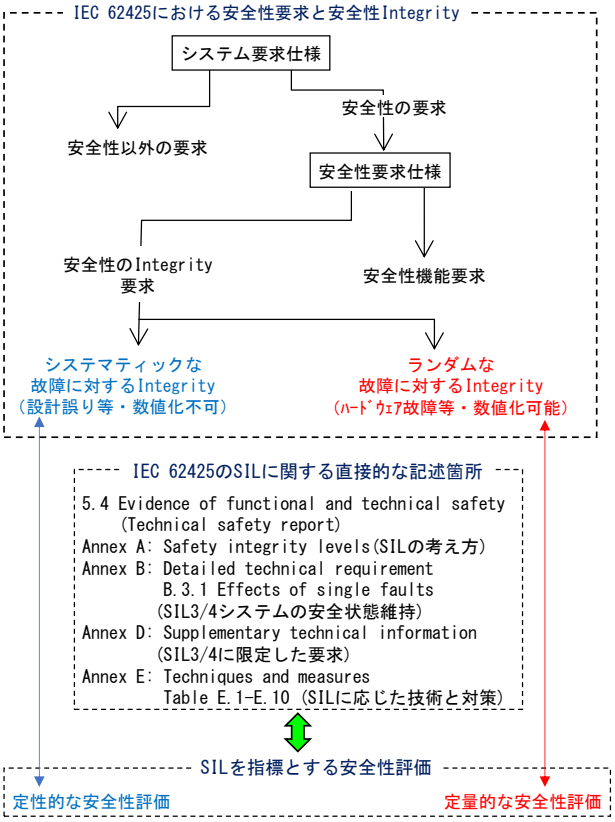

図 2　IEC 62425 のシステム要求と安全要求[2]

３．２．安全性の確保の考え方

従前の安全性評価においては、マネジメント等の定性的な面を考慮しながらも、システム、サブシステム又は装置単位の許容ハザード発生率（THR: Tolerable Hazard Rate (/h)）等、定量的な側面と、類似の既存システムの技術的手法との比較によるものであった[1]。しかしながら、IEC 62425 では、SIL の達成には、レベルに応じた品質管理条件、安全管理条件、技術的安全条件及び定量化された安全性目標の遵守が要求されている[2]。また SIL は装置等ではなく安全関連機能に割り当てられると規定されている。IEC 62425 に記述される、SIL の割当ての手順を図 3 に示す[2]。まず対象システムに対してリスク解析を行ってハザードログを作成し、認識された各ハザードのサブシステムの個別機能への割当てを行うことによってシステム機能としての THR が決定される。そして、表 1 に示すように、SIL Table に沿って、THR に応じて要求される SIL が決定される。これに基づいてサブシステムの THR と SIL が設定されると共に、ハザード発生率が各要素に割り当てられ、各要素の SIL と機能故障率（/h）が設定される。

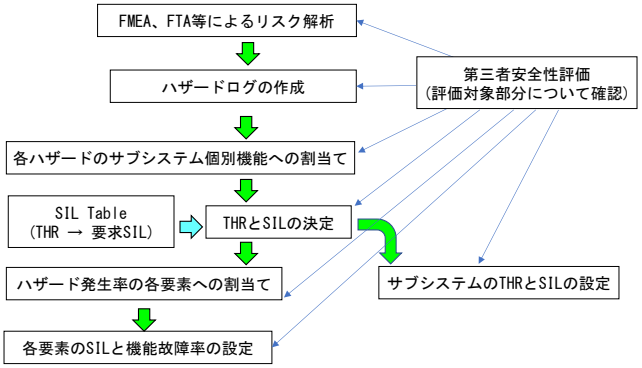

図 3　THR と SIL の割り当て[2]

表 1　SIL Table (THR に応じて要求される SIL)[2]

許容可能なハザード発生頻度（THR:1時間／1機能当たり）	要求されるSIL (Safety Integrity Level)
$10^{-9} \leqq THR < 10^{-8}$	4
$10^{-8} \leqq THR < 10^{-7}$	3
$10^{-7} \leqq THR < 10^{-6}$	2
$10^{-6} \leqq THR < 10^{-5}$	1

IEC 62425 によれば、本来はこのような手法で導出される SIL が、実際には鉄道事業者等の要求として例えば信号システムが SIL4 と設定される事例が多い。これらの過程に必要な作業の一部（リスク解析等）は、安全性評価の対象となるが、IEC 62425 では THR に応じて SIL が割り当てられるように記述されていることに留意し、整合を図ることが望ましい。

３．３．FTA に関する検討

３．３．１．機能の独立性と共通原因故障

安全性評価のために、主要なリスク解析手法として FTA が行われるが、複数の故障モードの共通原因となる故障（共通原因故障）が存在する場合、それらの故

障モードを入力事象とする複数のツリー中の AND ゲート又は OR ゲートに独立して共通原因故障を設定してしまい、その結果、誤ったハザード発生率を算出する可能性があると考える。図 4(上)に、その例を示す。IEC 62425 では、このような共通原因故障を重視し、それに関して詳細に記述している。この例では、図 4(下)に示すように、共通原因故障は別のツリーに配置し、OR ゲートで繋ぐことが妥当である [2]。このように、共通原因故障の扱いは、安全性評価の FTA においても、IEC 62425 の記述を意識して十分に注意すべきであると考える。

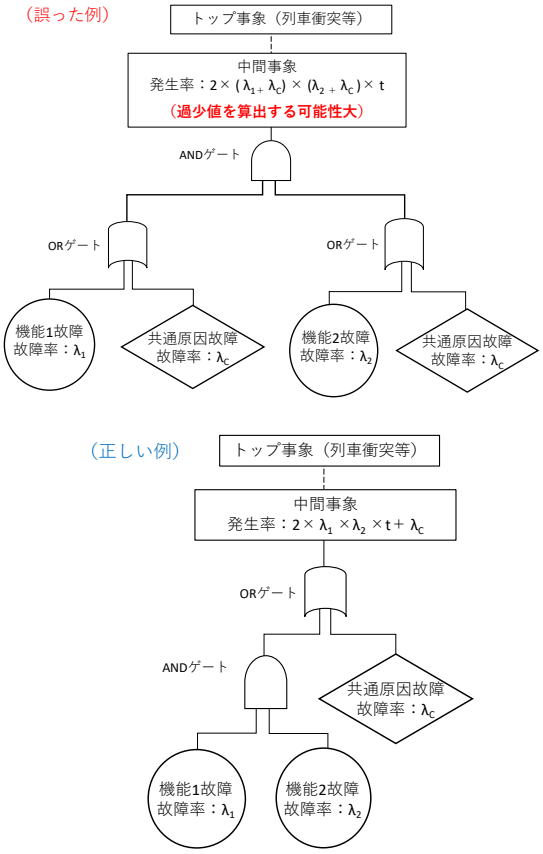

図 4　共通原因故障を含む FTA の例 [2]
((上)：誤　(下)：正)

3．3．2．フェールセーフ性の確保

IEC 62425 B.3.1 には、フェールセーフ性（Fail safety）の達成方法として、Composite（複合型）fail safety、Reactive（反応型） fail safety 及び Inherent（本質型）fail safety の 3 種類が挙げられている [2]。それらの概念は、FTA においては、以下(1)～(3)に示す通り、時系列的な事象は再現できないものの、部分的なツリー（FT）として表すことができると考える。このことから、(1)～(3)の FT モデルが Composite fail safety、Reactive fail safety 又は Inherent fail safety から導出される場合は、フェールセーフ性が確保されるとの判断が可能と考える。

(1) Composite fail safety

概念を図 5 に示す。独立した安全関連機能 A/B が論理積（AND）で結合されたモデルにおいて、機能 A に危険側故障が生じた場合、十分に短い時間内の検知(Detection)と否定(Negation)により、続いて機能 B に危険側故障が発生しても錯誤出力をせず、安全状態を保つという概念である [2]。この例では各々の検知、否定の機能も独立であると仮定する。

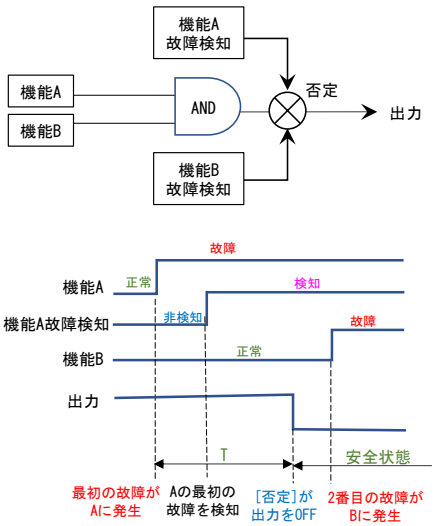

図 5　Composite fail safety の概念 [2]

Composite fail safety の概念に対応すると考える FT のモデルを図 6 に示す。機能 A /B の危険側故障を基本事象、それらを直上の AND ゲートの入力事象、「故障検知・停止」を制約ゲートとする [1]。

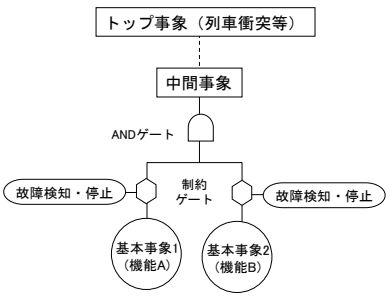

図 6　Composite fail safety に相当する FT モデル

このモデルでは、機能 A/B に同時に危険側故障が生じて AND ゲートから錯誤的な出力がされる事象がハザードであり、その防止策が「故障検知・停止」であるため、図 5 に示す Composite fail safety の概念に相当すると考える。

(2) Reactive fail safety

概念を図 7 に示す。1 つの安全関連機能で構成されるモデルにおいて、その機能に危険側故障が生じた場合、十分に短い時間内で検知（Detection）、否定（Negation）することにより、錯誤出力を回避し安全状態を保つという概念である [2]。

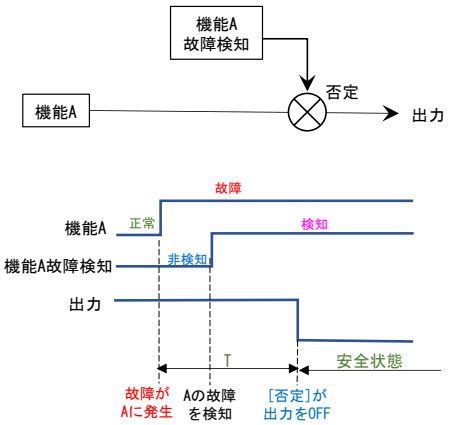

図 7　Reactive fail safety の概念 [2]

Reactive fail safety の概念に相当すると考える FT のモデルを図 8 に示す。機能 A の危険側故障を基本事象、「故障検知・停止」を制約ゲートとするこのモデルでは、機能 A に危険側故障が生じて錯誤的な出力がされる事象がハザードであり、その防止策が「故障検知・停止」であるため、図 7 に示す Reactive fail safety の概念と合致すると考える。

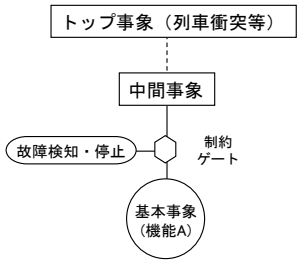

図 8　Reactive fail safety に相当する FT モデル

(3) Inherent fail safety

単一アイテム上の安全関連機能に起こり得る全ての故障モードがハザードに至らない、という条件下で認められる概念である。この条件は IEC 62425 Annex C で定義される手続を採用することにより正当化される [2]。Inherent fail safety の概念に対応する FT としては、1 つの機能の危険側故障を基本事象とし、その上方に制約ゲート、AND ゲート等が無い単純なモデルが考えられる。このモデルでは、機能自体が本質的なフェールセーフ性を備え、その危険側故障率が十分に低いことが、ハザードの防止策となる。

3．4．FMEA に関する検討

FMEA においては、要素毎に、機能、故障モード、原因、影響、重大さ、頻度、リスク等が検討される。また開発の各段階で検討されたリスク低減の対策が反映された FMEA が繰り返されることにより、リスクが受入可能となるまでの対策効果が評価される [1]。一方、IEC 62425 Annex E 及び Annex C には、系統的故障及び偶発的故障の防止、低減のための技法と対策（Techniques and measures）が記述されている [2]。この技法と対策は、表 2 に示すように、FMEA の結果表に追記された「対策」に相当すると考えられるため、FMEA に活用することが望ましいと考える。

表 2　FMEA と IEC 62425 Annex E Technique & Measures（例）の対応 [2]

FMEAの例

要素	機能	故障モード	故障原因	故障の影響	対策	重大さ	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	高信頼装置の採用 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
：	：	：	：	：	：	：	：	：

IEC 62425 Annex E Technical Measures の例（Table E.5 - Design features抜粋）

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4
1 Protection against operating errors	R: plausibility checks on each input command		HR: plausibility checks on each input command	
2 Protection against sabotage	–		R: additional organisational measures are necessary	
3 Protection against single fault for discrete components	R: all hazardous failure modes to be either detected and negated or demonstrated to be inherently safe such as a result of inherent physical properties		HR: all hazardous failure modes to be either detected and negated or demonstrated to be inherently safe such as a result of inherent physical properties	
：	：	：	：	：

4．おわりに

当研究所が行ってきた安全性評価と、鉄道関係の国際規格である IEC 62425 の接点について考察し、前者に後者の考え方を採り入れ、整合を図る場合の留意点を整理した。今後、安全性評価と IEC 62425 の他の項目、さらに IEC 62425 以外の国際規格との接点について考察し、国際規格との整合性について引き続き検討していきたい。

参考文献

1)　林田他，"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"，交通安全環境研究所ﾌｫｰﾗﾑ 2017 講演概要集 pp11-14

2)　IEC 62425 Edition 1.0 2007-09