① 鉄道信号システムの設計安全性評価に関する新たな取組

交通システム研究部　※林田 守正　佐藤 安弘　竹内 俊裕

1．まえがき

本報では、海外向け鉄道システムの設計段階を主な対象とする第三者としての安全性評価に関し、交通安全環境研究所がこれまでに取りまとめた評価報告書の標準的な構成・内容の提案に基づき、IEC シリーズをはじめとする国際規格との調和や規格適合性評価等との関連について、さらに検討を深めた結果を報告する。また、鉄道システムの高度化、複雑化への対応の一環として、新しい評価手法である STAMP (System Theoretic Accident Model and Processes）や、近年重要性が増しているセキュリティ評価への取組について述べる。

2．第三者安全性評価と国際規格

2．1．安全性評価報告書の標準的な構成（案）

前報 [1]で提案した第三者安全性評価（以下、「安全性評価」という。）の報告書の標準的な構成を図 1 に示す。中心的な記述事項は「安全性(S)に関する評価結果」であるが、安全性担保の前提条件として、「信頼性等(RAM)に関する評価結果」も記述する。また、評価対象範囲、参照資料、用語／略語の定義、対象システム概要、評価方法等についても記述する。

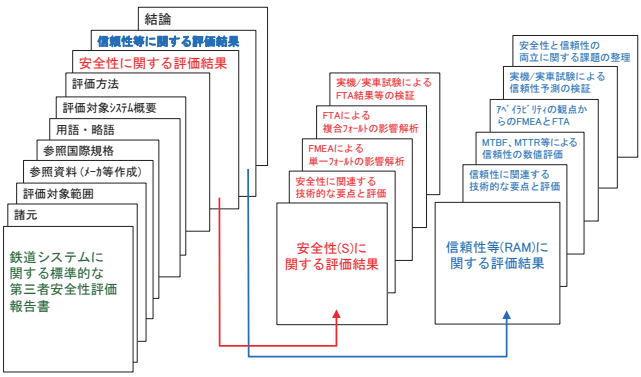

図 1　第三者安全性評価報告書の構成案 [1]

2．2．参照する国際規格

安全性評価報告書の記述に際して参照する国際規格を表 1 に例示する。その中で、IEC 62425 及び IEC 62278 を重点的に参照し、整合を図ることとする。特に、2.1.に前述した構成は、IEC 62278 に規定される RAMS （ Reliability, Availability, Maintainability and Safety）の概念に基づくものである [2]。

2．3．第三者安全性評価の位置付け

IEC 62425 によれば、システムの安全性の承認には、「Independent Safety Assessment」(以下、「ISA」という。）の実施が必須であるとされる。また安全性の証拠文書としては以下の 4 編が挙げられている [3]。

- System Requirement Specification (ｼｽﾃﾑ要求仕様書)
- Safety Requirement Specification (安全性要求仕様書)
- Safety case（セーフティケース：Part 1～Part 6）
- Safety assessment report（安全性評価報告書）

2.1 で前述した第三者安全性評価は、上記の「ISA」に該当すると考えられる。また、その評価の参照文書は「Safety case」の Part 4（Technical Safety Report）の内容又はその関連資料であり、評価報告書は、上記の 4 つの証拠文書の 1 つである「Safety assessment report」に該当すると考えられる。

表 1　参照する国際規格（例）

規格番号	規格の概要
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 62278	鉄道におけるRAMS
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（電磁両立性）

2．4．安全性評価への国際規格の考え方の反映

2．4．1．安全性の水準

IEC 62425 においては、安全性の水準として、非安全事象の発生頻度に基づいて 4 段階の SIL（System Integrity Level）が定義されており、その最高水準は SIL4（1×10^{-9}/h～1×10^{-8}/h）とされている [3]。これは主にハードウェアの非安全側故障率に基づくものである。一般的に鉄道の列車制御システムや信号システムには SIL4 が要求されるため [4]、各要素又はシステム全体における非安全事象の発生頻度が SIL4 を満足するか否かを主要な判断基準とする。一方、IEC 62278 には、リスクの受入れについて、ALARP（現実的に可能な限り低いこと）、GAMAB（全体として少なく

とも既存のものと同等の安全性）及び MEM（死亡事故のリスクが最も少ないこと）の 3 つの原則が示されている [2]。このうち、日本の鉄道システムは世界的にも非常に高い安全性の実績を有していることから、GAMAB の原則を採り入れることが適切であると考える。しかし、ALARP や MEM の原則を採り入れていくことも今後の課題であると考える。

２．４．２．リスクの定義

「リスク」という用語は、一般的には漠然とした危険性という意味合いで使われることが多いが、IEC 62278 等では、「非安全事象の発生頻度」と「非安全事象による影響の深刻さの程度」のマトリクス（行列）で定義される指標であるとされる [2]。そこで、上記の「発生頻度」と「影響の深刻さ」を点数化し、その積としてリスク値を算出し、予め設定した閾値との比較で可否を判断するべきであると考える。

２．４．３．ソフトウェアの安全性

ソフトウェアの誤りに起因する非安全事象は、ハードウェア故障に起因する事象とは異なり、偶発的に発生することは無いが、誤りが潜在していれば必然的に発生する。当研究所では、ソフトウェアの安全性については、主に設計資料のフローチャート、データフロー図、シーケンス図等を確認することにより評価を行ってきた。しかし、近年のシステムのソフトウェアは大規模化、複雑化が著しく、プログラムの細部まで確認することは非常に困難である。IEC 62279 には、ソフトウェア開発に関する技術や手法等が規定されている。また、2.4.1 で前述した SIL とは異なるソフトウェア SIL（SIL0～SIL4）が定義され、レベル毎に、個別の技術や手法の推奨が 3 段階（推奨しない、推奨する、大いに推奨する）で示されている [5]。そこでソフトウェアについては、直接的な確認が可能な技術内容の他、全般的に IEC 62279 に定められているような開発手法や検証体制に基づいて製作されていることを確認することが適切であると考える。

２．４．４．ノイズの影響

ノイズの影響による非安全事象は再現性が乏しく、また、システムが使用されるノイズ環境に大きく左右される。従って、ノイズの影響に対するシステムの安全性については、耐性や対策技術を含め、一意的な可否の判断が難しい。そこで、システムが IEC 62236 シリーズに規定される条件や方法に準拠した EMC（電磁両立性）に関する試験を受け [6]、試験結果が要件を満足していることを確認するとともに、システムが使用されるノイズ環境がその試験条件の範囲内であることを確認することが適切であると考える。

３．規格適合性評価との関係

３．１．安全性評価と規格適合性評価との対比

近年は、メーカ等が鉄道システムの輸出に際し、その安全性を相手先に証明する方法として、表 1 に示したような機能安全関連の国際規格への適合性について第三者評価や認証（以下、「規格適合性評価等」という。）を受けることが一般化している。第三者による安全性評価と規格適合性評価等との対比を表 2 に示す。後者の主眼は技術の内容よりも、むしろ製品に対する安全マネジメントのプロセスであるといえる。

表 2　第三者安全性評価と規格適合性評価／認証 [1]

	第三者安全性評価 （主に設計安全性）	規格適合性評価／認証 （機能安全関連）
評価の主眼	・システムの技術内容、設計仕様等	・システム（製品）に対する安全マネジメントのプロセス
評価の指標	・各国の安全性に関する基準 ・非安全事象の発生頻度 ・既存システムと同等以上の安全性 ・各種国際規格の規定（SILの定義、耐ノイズ性、ソフトウェア安全性等） ・その他	・対象とする国際規格（IEC等）の各条文に対応する証拠文書の存在および記述の適合性
国際展開において第三者評価が活用されるケース	・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）。 ・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規格適合性評価報告書／認証書相当と判断することが前提）。	・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。
第三者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。 ・当研究所鉄道認証室は認定機関による認定を取得している。

2.3 に前述した解釈とは異なるが、この規格適合性評価等が IEC 62425 に記述される「ISA」に該当すると解釈することも可能であると考えられる。その解釈によれば、対象規格が IEC 62425 であれば、評価の参照文書はセーフティケースの全ての内容であり、2.1 に前述した安全性評価は、必要に応じて規格適合性評価等を補強する目的で実施され、安全性評価報告書は規格適合性評価報告書等の補足文書として添付されるという位置付けが考えられる。この場合は、安全性評価報告書と規格適合性評価報告書等との間で、参照資料や記述内容に関する整合性を担保することが重要となる。

一方、システムの導入先によっては、必ずしも規格適合性評価報告書等が無くても、安全性評価報告書のみが、ISA の証拠として採用されるケースも存在する。

３．２．安全性評価への規格適合性評価手法の導入

安全性評価において、直接的な技術内容の確認に基づく判断が困難な事項については、規格適合性評価等

の手法を部分的に採り入れていくことが適切であると考える。その一例として、2.4.3 で前述した、ソフトウェアの安全性に関する評価が挙げられる。データフロー図等の確認による評価と共に、直接的な確認が困難なプログラムの細部までを包含する全般的な安全性については、規格適合性評価等にならって、IEC 62279 に準拠した開発、検証体制を文書で確認することによって安全性が担保されていると判断することが適切であると考える。また、他例として、2.4.4 に前述したようなノイズの影響についても、IEC 62236 に準拠した EMC に関する仕様や試験結果を文書で確認することによって、安全性を評価することが適切であると考える。

4．新たな安全性評価手法／評価対象

4．1．STAMP の試行

2012 年に、サブシステム間の相互作用に着目した STAMP と呼ばれる新しい安全設計手法が米国で提唱された [7]。現代のシステムのアクシデントの多くはシステム構成要素の故障によって起きるのではなく、システムの中で安全のための制御を行う要素の相互作用が働かないことによって起きるというアクシデントモデルに基づく手法であり、従来の個別部品や機器ベースの故障解析である FMEA（Failure Mode and Effects Analysis）や FTA（Fault Tree Analysis）とは異なる発想である。鉄道分野においても、高度化・複雑化したシステムのリスク評価に対応するには、FMEA や FTA に加え、STAMP の活用が有効であると考えられる。鉄道分野での STAMP の応用としては、踏切制御装置への適用例が公表されているが [7]、本報では、図 2 に示すような、簡単な連動装置をモデルとして試行した。制御を行う要素（Controller）を連動装置、制御される要素（Controlled process）を転てつ機と仮定し、制御構造図を図 3 に示すように構築した。連動装置から転てつ機への制御指示は、定位への転換、反位への転換、鎖錠及び解錠とし、各々の制御指示について連動装置へのフィードバック機能を有することとした。また、それ以外の関係要素として、進路構成、軌道回路（3 区間）及び信号機（出発／場内）を挙げた。

それに基づき、表 3 に示すように、アクシデント、ハザード及び安全制約を整理し、表 4 に示すような、非安全な制御指示を抽出した。今後は、このようなモ

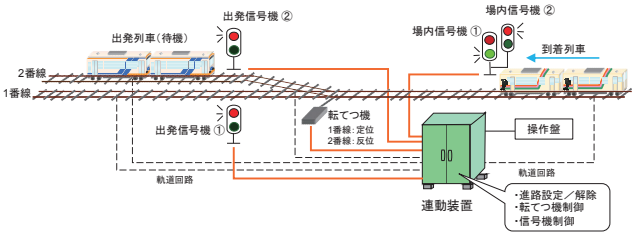

図 2　STAMP 試行の対象とした連動装置のモデル

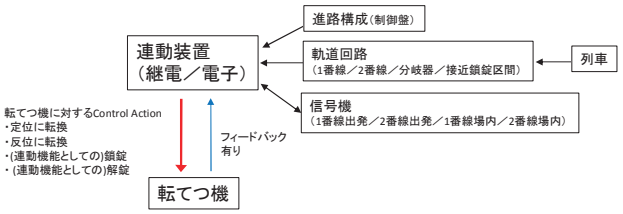

図 3　制御構造図の構築

表 3　アクシデント／ハザード／安全制約の整理

アクシデント	ハザード	安全制約
（A1）列車が分岐器上で脱線する	（H1）列車が分岐器上に在線中に不正転換する	（SC1）列車が分岐器上に在線中は転換してはならない
（A1）列車が分岐器上で脱線する	（H2）列車が分岐器上を走行中に鎖錠されない	（SC2）列車が分岐器上に在線中は鎖錠しなければならない
（A1）列車が分岐器上で脱線する	（H3）列車が非開通の分岐器を背向で通過する	（SC3）列車が背向で分岐器を通過する際に非開通であってはならない
（A2）列車同士が衝突する	（H4）到着列車の進路が駅在線列車と競合する方向に分岐器が開通している	（SC4）進路が競合するように分岐器を開通させてはならない
所定の列車が駅から出発できない	・分岐器非開通の場合、解錠ができない ・分岐器非開通の場合、定位または反位への転換ができない ・分岐器開通後の鎖錠ができない	所定の出発ができるよう解錠、転換、鎖錠を行う
所定の列車が駅に到着できない	・分岐器非開通の場合、解錠ができない ・分岐器非開通の場合、定位または反位への転換ができない ・分岐器開通後の鎖錠ができない	所定の到着ができるよう解錠、転換、鎖錠を行う

デル適用の妥当性を検証したうえで、非安全な制御指示に至るシナリオを想定し、非安全な制御指示の原因を特定して対策を講じる、という段階に進めていく。また、他のシステムへの適用についても検討する。

表 4　非安全な制御指示の抽出（赤字：非安全事象）

制御指示	与えられないとハザード	与えられるとハザード	早すぎ／遅すぎ／誤順序でハザード	早すぎる停止／長すぎる適用でハザード
反位から定位に転換指示	・1番線の発着が不可 ・1番線から誤出発すると脱線	・列車が分岐器上に在線すると脱線 ・2番線から誤発車すると脱線	早すぎると ・1番線からの列車より先行する2番線からの列車の出発が不可 ・1番線からの列車出発前の2番線への列車到着が不可 ・1番線への列車に先行する2番線への列車の到着が不可 ・2番線への到着列車が分岐器直前だと1番線に誤進入（1番線に他列車在線だと衝突） ・2番線への到着列車が分岐器上だと脱線 ・2番線からの出発列車が分岐器上だと脱線 遅すぎると ・1番線からの出発が遅延 ・1番線への到着が遅延	早すぎる停止だと ・転換が途中で停止し列車の発着が不可 長すぎる適用だと ・次の反位への転換が不可
定位から反位に転換指示	・2番線の発着が不可 ・2番線から誤出発すると脱線	・列車が分岐器上に在線すると脱線 ・1番線から誤出発すると脱線	早すぎると ・2番線からの列車より先行する1番線からの列車の出発が不可 ・2番線からの列車出発前の1番線への列車到着が不可 ・2番線への列車に先行する1番線への列車の到着が不可 ・1番線への到着列車が分岐器直前だと2番線に誤進入（2番線に他列車在線だと衝突） ・1番線への到着列車が分岐器上だと脱線 ・1番線からの出発列車が分岐器上だと脱線 遅すぎると ・2番線からの出発が遅延 ・2番線への到着が遅延	早すぎる停止だと ・転換が途中で停止し列車の発着が不可 長すぎる適用だと ・次の定位への転換が不可
鎖錠指示	・車両が分岐器上を走行中だと脱線	転換が不可	遅すぎると ・分岐器に進入した車両が脱線	早すぎる停止だと ・分岐器に進入した車両が脱線 長すぎる適用だと ・次の解錠、転換が不可
解錠指示	・転換が不可	車両が分岐器上を走行中だと脱線	早すぎると ・分岐器から進出前の車両が脱線	早すぎる停止だと ・解錠が不完全で次の転換が不可 長すぎる適用だと ・次の鎖錠が不可

4．2．セキュリティ評価について

列車制御等の安全関連の通信のセキュリティについても、関連国際規格との整合や、4.1 で前述した STAMP の活用を考慮した評価手法を検討する必要があると考える。例えば CBTC（Communication Based Train Control）においては、図 4 に示すように、列車が自ら取得する位置情報が無線通信を介して車上装置と地上装置の間で伝送され、それに基づいて列車間隔制御等が行われる。したがって、例えば先行列車位置データが人為的に、あたかも実際より前方に在線するか、又は、在線しないかのように改竄された場合は、後続列車が先行列車に追突する危険性が生じる。そのため、安全性評価項目として無線のセキュリティが不可欠であることから、伝送系やセキュリティ関連の国際規格（IEC 62236 シリーズ、IEC 62280 等）を参照しながら、表 5 に示すような偶発的又は人為的な脅威とその防止技術の評価手法について [8]、ケーススタディを含めた検討を始めている。また、従来の RAMS 評価手法へのセキュリティの適用方法や、STAMP を活用した新たな通信セキュリティ評価方法についても検討するとともに、わが国における列車制御通信のセキュリティが、国際規格への適合のみで担保されるかどうかについて、STAMP を活用した解析を含めて、妥当性を検討する予定である。

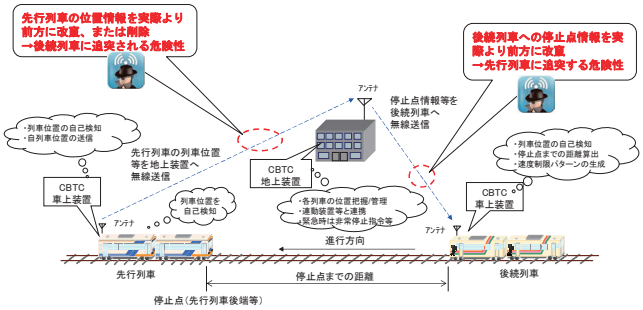

図 4　CBTC におけるセキュリティの人為的脅威

表 5 伝送系の脅威と対策 [8]

脅威	通番	タイムスタンプ	タイムアウト	送信元／受信先ID	フィードバックメッセージ	同一証明手順	安全コード	暗号化技術
繰り返し	○	○						
削除	○							
挿入	○			○	○	○		
再順序	○	○						
劣化							○	○
遅延		○	○					
なりすまし					○	○		○

5．おわりに

(1)当研究所が実施してきた第三者安全性評価について、IEC シリーズ等の国際規格の規定に基づく位置付けを整理し、また、国際規格の評価への反映について考察した。

(2)安全性評価と規格適合性評価等との対比や関連性を考察し、安全性評価に規格適合性評価の手法を導入した例を示した。

(3)新しい評価手法である STAMP や、重要性が増しているセキュリティに関する取組の状況を紹介した。

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 62278 First edition 2002-09 英和対訳版
3) IEC 62425 Edition 1.0 2007-09
4) 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
5) IEC 62279 Edition 2.0 2015-06
6) IEC 62236-1～5 Edition 2.0 2008-12
7) "はじめての STAMP/STA" Ver.1.0, (独)情報処理推進機構（2016）
8) IEC 62280 Edition 1.0 2014-02