

① 第三者安全性評価と規格適合性評価の併存について

交通システム研究部 ※林田 守正 佐藤 安弘 竹内 俊裕 工藤 希 渡邊 翔一郎
 鉄道認証室 長谷川 智紀 森 裕貴
 東京大学 水間 毅

1. はじめに

当研究所はこれまでに、国内外向けの鉄軌道システムに対する第三者安全性評価を数多く行ってきた。しかし近年、海外においては、鉄道関連のメーカ等が自社システムの安全性を導入先に対して証明する手段として、同じく第三者による国際規格（IEC (International Electrotechnical Commission, 英) シリーズ等）への適合性評価を受け、認証書を取得すること（以下、認証手続の有無に係わらず「規格適合性評価」という。）が主流になっている¹⁾。このような状況を踏まえ、規格適合性評価との併存を念頭に置いて、技術的な検討を主体とする第三者安全性評価の課題や方向性について考察した結果を述べる。なお、規格適合性評価も広義の安全性評価に含まれると考えられるため²⁾、本報告では安全性評価又は規格適合性評価を実施する第三者を「ISA (Independent Safety Assessor)」と総称する。

2. 第三者安全性評価の形態

日本の鉄道技術が国内外に導入される際、導入先の鉄道事業者（以下、「事業者」という。）がシステム受入れの妥当性を判断するために、第三者安全性

評価が必要とされる形態を、当研究所の実施事例に基づいて図1に示す³⁾。[ケース1]は国内導入のケースである。事業者が十分な技術力によってシステムインテグレータを務め、技術基準等による他、自社のノウハウに基づいてシステム受入の妥当性を判断する。ただし、技術の新規性が高い場合等には第三者安全性評価が要求される。[ケース2]及び[ケース3]は海外での導入のケースである。[ケース2]は、[ケース1]と同様に技術力を有する事業者がシステム受入の妥当性判断を行うが、その判断材料の1つとして第三者安全性評価が要求されるケースである。[ケース3]は、技術ノウハウが少ない事業者が、第三者機関（鉄道技術コンサルタント等）に、技術力を要する業務を委託するケースである。この場合、事業者から委託された第三者機関（以下、「事業者側ISA」という。）により、システムの安全性の証明（主に規格適合性評価、場合により安全性評価も）が要求される。事業者側ISAはそれらの評価報告書を他の技術文書等と共に精査したうえで、システム受入れの妥当性を判断する。

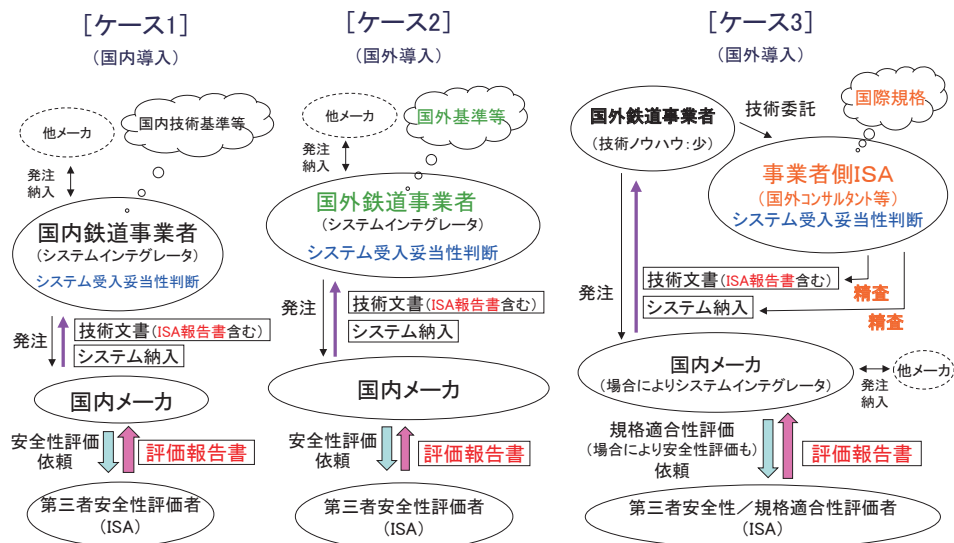


図1 第三者安全性評価の形態³⁾

3. 安全性評価と規格適合性評価の併存について

3. 1. 国外向けシステム評価における併存状況

当研究所における国外向けシステムに対する安全性評価は、2. で前述したように、[ケース 2] 及び [ケース 3] の形態で実施されている。[ケース 2] では、安全性評価報告書が国外の事業者により、規格適合性評価報告書や認証書に代わるものとして扱われ、システム受入れ可否の判断材料の一部とされる。ただし、実態として、該当する国や事業者は極めて限られている。[ケース 3] では、規格適合性評価のみが実施される事例が多いが、安全性評価が並行して実施される事例も存在する。3.2. に後述するように、規格適合性評価だけではリスク解析の妥当性評価が困難な事例も少なくないを考える。したがって、非安全事象の発生の可能性を最小限に留めるためには、今後も、技術内容に關与する安全性評価の意義は小さくないと考える。本報告では、主に [ケース 3] において、安全性評価が規格適合性と併存していくための方策を考察した。

3. 2. 評価実施面での比較

[ケース 3] において、同一のシステムに対し、安全性評価及び規格適合性評価が実施されるケースでの、両者の実施面での性格を表 1 に示す。

表 1 安全性評価と規格適合性評価の実施面での比較

	第三者安全性評価 (主に設計安全性)	規格適合性評価 (機能安全関連)
評価の主眼	・システムの技術内容	・システムに対する安全マネジメントのプロセス
評価のために提示される文書	・[参照文書] (安全性の判断の根拠) ・システムの基本設計資料 ・システムの新規性、安全性等を示す技術資料 ・システムのリスク解析資料	・[評価文書] (文書自体が評価対象) ・適用する国際規格 (例: IEC 62425 等) ・システムが当該国際規格の各条文に適合していることを証明する各種文書 (文書自体が評価対象)
検討項目	・新技術要素の基本設計の妥当性 ・SIL等の指標に沿ったリスク分析に基づく定量的な安全性 ・従来システムとの安全性の比較 ・システムの維持管理に依存する定量的な安全性	・システムの当該国際規格への適合性を証明する各文書の記述内容の妥当性
可否判断の指標 (例)	・SILで規定される安全性 (SIL4等) ・従来システムと同等以上の安全性	・当該規格の全ての条文への準拠 (評価対象文書上の記述の確認)
成果物	・安全性評価報告書 (規格適合性評価参照文書の一部とされる場合あり)	・規格適合性評価報告書 ・認証書
第三者評価機関としてのオーソライズの仕組み	・国内外におけるオーソライズの仕組みは特に無し	・認証機関に対する要求事項に関する国際規格 (ISO/IEC 17065) への準拠 ・認定機関による製品認証機関としての認定 (上記準拠と共に取得済)

安全性評価の主眼はシステムの技術内容であり、判断の指標は、SIL (Safety Integrity Level, 英) 等の指標で要求される定量的な安全性 (例えば SIL4: 非安全事象の発生頻度が $1 \times 10^{-9}/h \sim 1 \times 10^{-8}/h$) の担保の可否等と

考える。これに対し、機能安全関連の規格適合性評価の主眼は、システムに対する安全マネジメントのプロセスであり、判断の指標は、当該規格の全ての条文への準拠の有無であると考えられる。

また評価のために委託元から提示される文書は、安全性評価ではシステムの安全性の判断材料であるが、規格適合性評価では文書の存在及び記述そのものが評価の対象である。このように、安全性評価と規格適合性評価の性格は大きく異なるが、前者の成果物である安全性評価報告書が、後者の評価対象文書の一部として扱われることとなる。

3. 3. 評価対象及び成果物の関連性

3.2 で前述したように、[ケース 3] においては、安全性評価報告書が規格適合性評価の対象文書の一部として扱われ、その記述内容が規格適合性評価報告書の記述にも反映されるという事例が存在する。このような事例で、安全性評価及び規格適合性評価 (IEC 62425 の例) が並行して行われる場合の、双方の評価範囲の包含関係を図 2 に示す。

規格適合性評価の対象は「Safety Case」と呼ばれる一連の文書である。一方、安全性評価の対象は「Safety Case」の一文書である「Technical Safety Report」またはその付帯文書である各種の技術文書によって説明される技術内容である。そして、安全性評価の成果物である報告書は、「Technical Safety Report」の付帯文書として、「Safety Case」に含まれ、規格適合性評価の対象文書の一部となる。

IEC 62425 によれば、「Safety Case」及びその規格適合性評価報告書の他、「System Requirement Specification (システム要求仕様書)」等を含めた全ての文書が、事業者によるシステム受入れの安全面での妥当性判断、すなわちシステムの安全性承認に必要な証拠文書とされる²⁾。

[ケース 3] においては、図 1 及び図 2 に示すように、事業者側 ISA が事業者に代わり、これら全ての証拠文書を精査する。したがって、[ケース 3] において、同一システムに対し安全性評価と規格適合性評価が並行して実施された場合、規格適合性評価報告書だけでなく、安全性評価報告書も事業者側 ISA の精査の対象に含まれることとなる。

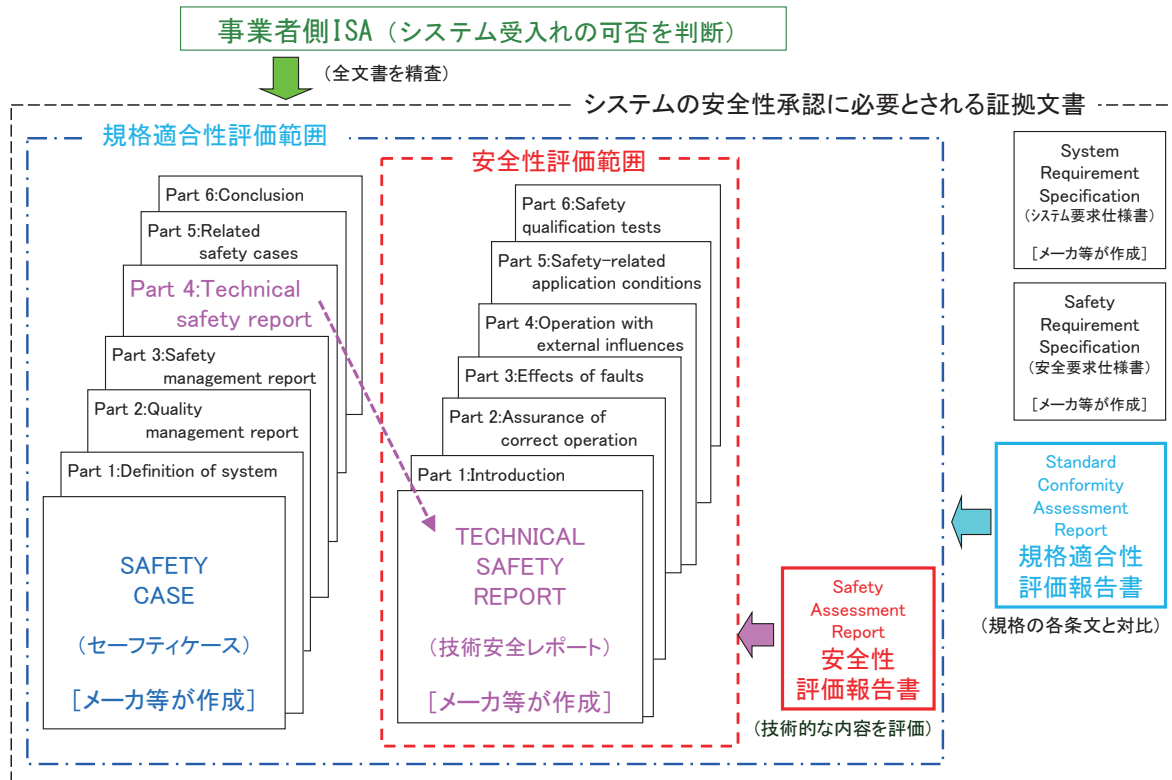


図2 安全性評価と規格適合性評価の範囲 (IEC 62425 の例)

3. 4. 今後の併存に向けた課題と対策

3. 4. 1. 規格適合性評価報告書の全般的な整合

3.3に前述したようなケースでは、事業者側ISAが、安全性評価報告書と規格適合性評価報告書を見比べながら精査すると考えられる。もし両報告書の記述内容に整合性が不十分な点が残っていると、それを事業者側ISAに指摘され、妥当性判断に支障をきたす可能性が生じる。このような事態を回避するため、両報告書の作成に当たっては、記述の細部に至るまで整合性がとれ、矛盾点が残らないように留意することが必要であると考えられる。これは、規格適合性評価においては、複数の評価対象文書間のトレーサビリティが重視されるが⁴⁾、事業者側ISAの視点からは、このことが安全性評価報告書と規格適合性評価報告書の間にも要求されると推定することによる。ただし、両者の整合性を図る過程では、ISO/IEC 17065の規定(認証機関のシステム開発への関与、コンサルティング等の禁止)に当研究所が抵触しないことが必要である⁵⁾。

3. 4. 2. 参照文書

表1に示すように、安全性評価は規格適合性評価と性格が大幅に異なるため、その参照文書の多くは、規格適合性評価の対象文書とは別のものとなる。しかし

総合的な設計仕様書(FDR(Final Design Review, 英)等)や主要なリスク解析文書(ハザードログ、FMEA(Failure Mode and Effects Analysis, 英)、FTA(Fault Tree Analysis, 英)等)は双方の評価で共有することが望ましい。また安全性評価のために提示される、技術内容の詳細な説明のための文書は、書式や表現が多様化しがちであるが、できるだけ統一性を有し、また総合的な設計仕様書の項目との関連性が明確化されることが望ましい。

3. 4. 3. 評価項目の絞り込み

安全性評価では、システムの新規性や従来技術との差分等に注目するため、重点的に評価する項目を絞り込む場合が多い。このような評価項目の絞り込みに際しては、客観的な選定基準と選定理由を明確にする必要があると考える。また、仕様項目全体の中での位置付けを整理する必要がある。これに対し、規格適合性評価においては、当該規格の規定全般にわたり、評価文書に対して準拠の可否を判断していくため、評価項目を特に絞り込むことは無いと考える。

3. 4. 4. 報告書の構成

一般的に、安全性評価報告書には、定型的な文書構成は存在せず、評価の項目と結果を任意に並べた形と

することが多い。一方、規格適合性評価報告書には、ある程度定型的な文書構成が存在する。そのため、安全性評価報告書の構成は、規格適合性評価報告書や総合的な設計仕様書の構成との対応が分かりやすい形とすることが望ましい。

3. 4. 5. 報告書の記述

安全性評価報告書と規格適合性評価報告書で用いる用語や文体は、極力整合させることが望ましい。特に類義語（例えば「危険事象」と「非安全事象」）については、共通化が必要であると考え。ただし、判断の記述としては、規格適合性評価報告書と違い、安全性評価報告書では参照文書に基づいて断言できる事項は極めて限られるため、推定的な語調（「・・・問題は無いと考えられる。」等）が多用される。

3. 4. 6. 指摘事項と対応

安全性評価報告書には、指摘事項、対策及び対応状況について記述される事例が多い。この記述については、規格適合性評価の観点では、対応状況が全て「Close（了）」であることが必須である。すなわち、指摘と対策の必要性のみが記述された事項は「Open（未了）」と見なされ、規格不適合と判断される可能性があることに留意することが望ましい。また、指摘事項と対応に関する記述は、ハザードログの記述とも整合することが望ましい。

4. 第三者安全性評価の今後について

4. 1. 国内導入向け [ケース 1]

今後は、1980年代のように全く新しい鉄軌道システムが続出することはあまり期待できないものの、国内導入向けの安全性評価のニーズは一定数残ることが予想される。当面の間、国内導入向けのシステムには、国際規格適合の必要性は小さく、規格適合性評価も行われないと考えられる。しかし国外で開発され、規格適合性評価／認証済のシステムが国内に導入されるケースにも対応できるように、安全性評価に国際規格の考え方を積極的に採り入れていく方向になると考えられる。

4. 2. 国外導入向け [ケース 2]

安全性評価を規格適合性評価と同等のものとして扱う少数の国外事業者（技術力有り）をターゲットとする安全性評価のニーズは、当面の間は持続すると考えられる。ただし、将来的にはそのような事業者が要求する安全性証明手段が、規格適合性評価／認証へ移

行する可能性は否定できない。そのため、安全性評価は、3.4で前述した方向になると考えられる。

4. 3. 国外導入向け [ケース 3]

技術力が十分でない国外事業者に代わって事業者側 ISA がシステム受入れの妥当性を判断するこのケースでは、規格適合性評価が増加していく可能性が高いと考えられる。しかし将来的にも、技術内容を主眼とする安全性評価が、規格適合性評価と併存する必要性は残ると予想されるため、3.4で前述した方向になると考えられる。

5. まとめ

第三者安全性評価の実施形態について、当研究所の事例に基づき、3種類のケースに分けて整理した。また国際的なシステムの安全性証明手段としては規格適合性評価／認証が一般化している状況を踏まえ、国外導入先のケースにおける第三者安全性評価と規格適合性評価の併存に関する課題と対策について検討した。そのうえで、第三者安全性評価の将来に向けた方向性を考察した。

参考文献

- 1) 江國実, "鉄道認証室における最近の動向", 交通安全環境研究所フォーラム 2018 講演概要集, pp.15-16
- 2) IEC 62425 "Railway applications - Communication, signalling and processing systems- Safety related electronic systems for signalling" Edition 1.0 2007-09
- 3) 林田守正他, "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, pp.11-14
- 4) 長谷川智紀他, "鉄道製品に関する安全関連規格に対して適合するための留意点について", 交通安全環境研究所フォーラム 2018 講演概要集, pp.17-20
- 5) ISO/IEC 17065 "Conformity assessment - Requirements for bodies certifying products, processes and services" First Edition 1.0 2012-09-15