

②③ 軌道系交通システムの技術に関する安全性評価手法の国際化への対応と標準化への取り組み

交通システム研究領域
自動車安全研究領域
理事

※林田 守正
青木 義郎
水間 毅

廣瀬 道雄

大野寛之

長谷川 智紀

森 裕貴

1. はじめに

軌道系交通システムの設備機器や車両に関わる安全性については、急速な国際化の流れの中で、従来わが国には馴染みが薄かったリスクの数値管理等の概念を含む国際規格に適合した評価が求められる事例が増加している。本報告では、交通安全環境研究所（以下「当所」という）が、第三者安全評価者として実施している安全性評価に関する手法の、国際規格への対応を重視した標準化に向けた取り組みについて述べる。なお、ここでは第三者安全性評価者を ISA（Independent Safety Assessor）と位置付け、それによる安全性評価を「ISA 評価」と表すこととする。

2. 最近の安全性評価の状況

図 1 に、最近（平成 20 年度以降、鉄輪車両走行試験および索道関係を除く約 50 件）の当所による ISA 評価対象システムの種別の内訳を示す。

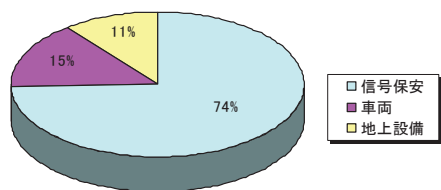


図 1 ISA 評価対象の種別（平成 20 年度以降）

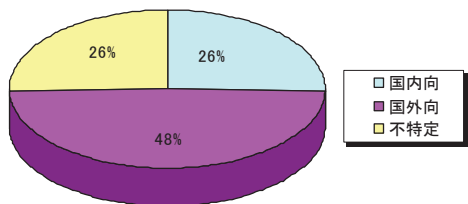


図 2 ISA 評価対象の展開先（平成 20 年度以降）

信号保安が全体の約 3/4 を占めるが、ホーム柵等の地上設備の評価例も出ている。図 2 に、評価対象事例の展開先の内訳を示す。国外向けが約半分を占め、国

内外を限定しない事例と合わせると約 3/4 が海外展開を意識したものである。本報告では、これらの ISA 評価事例をケーススタディとして検討を行った。

3. 評価手法の国際規格との整合

3. 1. 整合が必要な国際規格

鉄道に関する主要な国際規格としては、IEC（国際電気標準会議）規格、ISO（国際標準化機構）規格が挙げられる。そのうち、まず ISA 評価との整合の必要性が高い主要事項を多く含むと考えられる IEC 62278（RAMS）と IEC 62425（電子機器のセーフティケース）の 2 規格との整合について、検討することとした⁽¹⁾⁽²⁾。

3. 2. 整合に関する主な検討課題

3. 2. 1. ISA 評価の位置付け

IEC 62425 では、鉄道事業者側による安全性の承認前には、メーカー等が作成するセーフティケース等に加え、ISA 評価とその報告書が必須であると規定されている⁽²⁾。したがって海外展開事例では ISA 評価が必要条件として求められるケースが多いため、評価に当たっては ISA 評価の位置付けと役割を十分に認識する必要がある。特に報告書の記述は、ISA 評価と関連性が高いセーフティケース中の Part. 4 Technical Safety Report の記述との整合性を図る必要がある。

3. 2. 2. システムのライフサイクル段階

IEC62278 では 14 段階のシステムライフサイクルを規定し、その中で、総合セーフティケースは第 6 段階で作成すべきとされる⁽¹⁾。そのため、セーフティケースと併せて必要とされる ISA 評価においては、評価対象仕様が第 6 段階を含み、適合しているかどうかを確認し、その確認内容を報告書にも明記する必要があると考える。

3. 2. 3. SIL の概念

IEC 62425 では、リスクの数値管理の概念として、

SIL (Safety Integrity Level) を規定している⁽²⁾。これは図3に示すようなシステム要求、安全性要求の中で偶発的な故障に対する安全性の定量化を目的として、SIL1 (危険事象発生率: $10^{-6} \sim 10^{-5}/\text{hr}$) から SIL4 (同 $10^{-9} \sim 10^{-8}/\text{hr}$) を規定している。一般的に、信号保安システムの安全関連機能にはSIL4が要求される。日本の鉄道システムは実績としてSIL4より2桁以上高いレベルの安全性を実現してきたが、国際規格ではSIL算定の理論的な根拠の提示が求められるため、その対応が必要である。

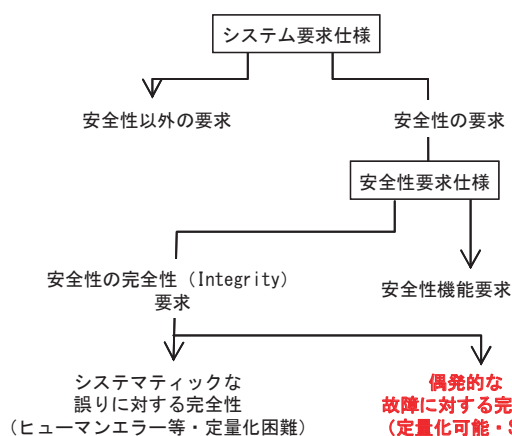


図3 システム要求仕様、安全性要求仕様と SIL⁽²⁾

4. ISA としての評価手法標準化へ向けた対応例

4. 1. 評価対象の展開先の区分

国内向けの事例では、国際規格への適合は求められず、鉄道事業者等が提示する安全性要件への適合性評価が求められるケースが多い。そのため評価手法の標準化に当たっては、完全な共通化をめざすよりも、評価対象の展開先の違いによって異なる部分を許容する方が適切と考える。ただし将来的な国際化の可能性も踏まえ、可能な限り共通化することが望ましい。

4. 2. 明確にすべき項目

4. 2. 1. 評価対象範囲

ISA 評価の内容や結果については依頼者のメーカ等に限らず、システム納入先に対しても責任が生じる可能性がある。したがって ISA 評価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 評価の対象外であり責任を負わない部分を明示する。

4. 2. 2. 用語、略語

IEC 62278 等の国際規格では、文書中の主な用語、略語の定義が明確にされている。これに倣って ISA 評価においても主要な用語、略語の定義を明確にする。

4. 2. 3. 参照資料

ISA 評価では評価の根拠となる参照資料として、前述のセーフティケース等の他、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。この場合参照資料に文書管理番号が無いと、ISA 評価完了後の資料特定が困難となり評価結果の再見が必要な場合に支障が生じると予想されるため、参照資料には全て文書管理番号が付与され、報告書に明示されることとする。

4. 3. FMEA と FTA

当所の ISA 評価では FMEA (Failure Mode Effects Analysis) および FTA (Fault Tree Analysis) を中核的な手法として用いてきた。一方、IEC 62425 では Technical Safety Report における単一異常影響 (Effects of single faults) および複合異常影響 (Effects of multiple faults) に対する安全性担保が規定され、FMEA を前者、FTA を後者の主要な解析手段として挙げている⁽²⁾。したがって FMEA、FTA による解析をこのような位置付けとするともに、FTA では図4に示すように、基本事象から頂上事象への到達を阻む制約ゲートの存在と信頼性 (SIL 等) を明確にすることで、安全性に対する評価を実施する。また、FTA は静的な事象解明には有意であるが、動的な事象解明には状態遷移図を利用した確率計算も行う。

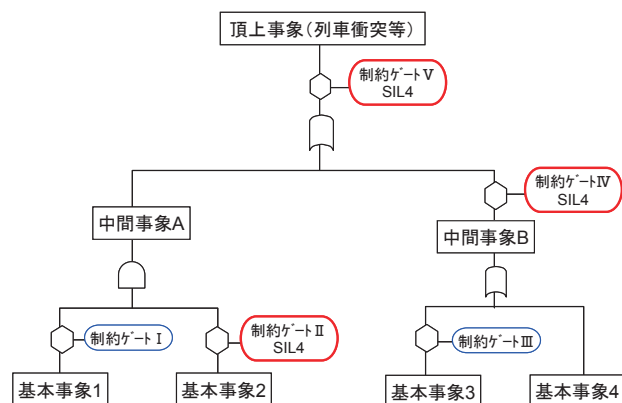


図4 FTA による複合異常影響解析と制約ゲート（模式図）

5. まとめ

当所（交通安全環境研究所）が ISA として実施してきた安全性評価の近況をケーススタディとし、評価手法の国際規格との整合を重視した標準化への道筋と、当所の独自手法について説明した。

参考文献

- (1) INTERNATIONAL STANDARD IEC 62278 対訳版 (2002)
- (2) INTERNATIONAL STANDARD IEC 62425 (2007)