システム安全の視点と列車制御・輸送管理システム

長岡技術科学大学　システム安全系　教授
東日本旅客鉄道株式会社　JR東日本研究開発センター　技術アドバイザー
平尾　裕司

システム安全の概念は、「The discipline that uses systematic engineering & management techniques to aid in making systems safe throughout their life cycle: Stephans（2004）」と定義される。このようなシステム安全では、絶対安全はなく、システムの開発から廃棄までの全ライフサイクルを通したリスク管理によってリスクを許容可能な水準以下に保つ考え方をとる。ここで、リスクとは危害が発生する確率とその被害の大きさの組み合わせである。

安全を確保するための方法は、1960年代に始まったアメリカ国防総省規格（MIL-STD-882）における方法を含め、化学プラント、機械など異なる適用分野を背景に成立したにもかかわらず、現在はリスク管理をベースとした方法に収斂したとみてよいであろう。代表的な例である機械安全の分野では、(1) 使用および予見可能な誤使用の明確化 (2) 危険源の同定 (3) リスクの見積もり (4) リスクの評価 (5) リスクの低減によってリスクアセスメントが行われる。この際のリスク低減方策として、(a) 本質安全設計 (b) 安全防護（隔離、停止）(c) 残留リスクについての使用上の情報の順で実施する3ステップメソッドがとられている。なお、(a) または (b) を適切に適用できる場合には、(c) で代替することは許されない。これらは、機械類の安全性に関する国際規格（ISO 12100）で規定されている。ヨーロッパ内では、安全に関わる製品・装置については、当該EU指令に適合することを第三者機関が検査および認証を行い、製造者がCEマークを貼付しなければならない。安全規格がEU指令の整合規格（指令の基本的要求事項を満足しているとみなされる規格）として引用される。

このように安全規格をベースとして、ヨーロッパでは、運用および保守も対象として事前にリスクアセスメントを行うことによって安全対策をとるとともに、使用者の側にも残留リスクを明示し、域内での製品・装置の自由流通を実現している。アメリカでは法制度の事情は異なるが、リスクに対する管理については、同様な取り組みが行われている。

日本におけるシステム安全の事情はどうであろうか。これまで法令へのコンプライアンスが主であり、事故等によって対策・指導が行われてきた。リスク管理では、リスクの許容水準は対象とするシステムから享受するメリットと残留リスクによるデメリット、コストで決まる。リスクは工学的には理解できても、絶対安全への期待が強い社会では、責任の範囲を含め、コンセンサスを得るのは必ずしも容易ではない。医療用ロボットなど先端技術を有するものの、その導入が日本ではむずかしい主要な理由になっているとの指摘もある。

平成18年4月には、労働安全衛生法が改正され、リスクアセスメントの実施が努力義務化された。これに伴って、今年7月には、リスク

Profile

略歴
博士（工学）

1953年	北海道出身
1973年	函館工業高等専門学校 電気工学科卒業
1973年	日本国有鉄道入社
1998年	財団法人鉄道総合技術研究所 列車制御研究室長
2003年	同　信号通信技術研究部長
2007年4月	長岡技術科学大学　システム安全系 教授
2007年6月	東日本旅客鉄道株式会社 JR東日本研究開発センター 技術アドバイザー

アセスメントを促進するための「機械の包括的な安全基準に関する指針」改正案が作成された。また、新技術へのリスクアセスメントの適用として、今年の4月には、「次世代ロボット安全確保ガイドライン案」が作成され、パブリックコメントの募集が行われた。原子力発電に関しては、すでに平成15年に原子力安全委員会が公開の安全目標（施設敷地境界付近の公衆の個人の平均急性死亡確率及びがん死亡確率）として　10^{-6}／年・サイトを示している。このように、日本においてもリスク管理に向けての取り組みが始まっているが、本格的に他分野にも浸透するには多くの時間がかかると予想される。

一方、日本国内で発生しているエレベータや遊戯施設の事故についてシステム安全の視点から見ると、報道で指摘されているメンテナンスの不備とは別に、全ライフサイクルを通してのリスク管理の重要性が明らかになる。上記リスク管理の基本的な考え方では、開発時の前提条件や同定された危険源は、設計のみならず、運用、保守に適切に反映され対策されなければならない。また、装置等に対する認証には、運用、保守の条件が含まれる。アメリカのある遊戯施設には、リスク管理による膨大な量の保守マニュアルが揃えられていると聞く。

列車制御・輸送管理システムの場合はどうであろうか。日本では、国鉄時代に電子連動装置が実用化され、鉄道信号のマイクロエレクトロニクス化安全性技術が確立された。その後、システムの高機能化に対応するために、鉄道事業者、メーカで共通に使用できる「列車保安制御システムの安全性技術指針」を鉄道総研が事務局となり、大学、鉄道事業者、メーカの協力のもとに1996年に作成した。本技術指針は、当時まだドラフト段階であった機能安全に関する国際規格（IEC 61508）をベースとして電子連動実現のために開発された安全性技術を取りまとめたもので、IEC 61508を本格的に適用した日本国内で最初のケースと考えられる。IEC 61508は、高度な機能を実現するために必要なコンピュータ制御における安全を対象とするもので、リスク管理によるコンピュータ制御のための安全要件を規定する重要な規格となっている。

このようなリスク管理の必要性のなかで、定量的な安全性評価のための努力も行われてきた。新たに開発する鉄道信号システムに対し、確率の数値だけに頼るのではなく、フェールセーフを原則として安全性確保の機構を組み込み、安全性技術・対策・プロセスが妥当なものであったかを確認する手段として定量的な安全性解析を位置付けした。従来の信号システムの危険側故障率の実績値との比較が当面妥当とした。2000年代になり、IEC61508をベースとしたいくつかの鉄道信号用IEC国際規格が新たに出現したが、安全性技術指針による経験のほか、電子連動開発当時にすでにMIL規格による安全管理について検討していたこともあり、鉄道信号分野では比較的早い対応ができたと考える。

現時点での課題として、リスク管理による国際規格に適合していることを示すためには、あるいは許容リスク水準が確保されていることを示すためには、どの程度のドキュメント、試験結果データが必要かつ十分か基準が明らかでないことが挙げられる。これは、システムの開発コストにも影響を与えることになるため、今後、重要な課題となると考えられる。海外の鉄道信号メーカでは、アセスメントのための費用が15億円を超えたともいう。このような状況のなか、今年6月に改定となったイギリス国防省規格（Def Stan 00-56: Safety Management Requirements for Defence System）では、安全手法を規定するのではなく、証拠（エビデンス）として提出されるドキュメント、試験結果のリスク管理上の確かさに重点を置く内容に変更されている。その確かさのレベルに応じて、要求されるエビデンスが異なり、定量的および定性的な2つのデータを求められることもある。Def Stanでは、これまでソフトウェアに関してフォーマルメソッドの適用を求めてきたが、エビデンス重視の方向によって必須事項ではなくなる。国際規格が、今後、適合性についてより踏み込んだ新たな展開になると予想される。今年の秋に開催されるコンピュータ制御の安全を扱う国際会議SAFECOMPのタイトルは、”Don’t claim it’s safe, show me！”である。

ヨーロッパでは、EU域内の鉄道の安全とインタオペラビリティを管理・推進するERA（European Railway Agency）が2005年に設置され、新たな展開を迎えている。安全に関して具体的には、共通安全目標（CSTs）、共通安全手法（CSMs）、共通安全項目（CSIs）を導入してリスク管理による安全確保を進めるとともに、事故データベースを構築して鉄道の潜在危険源の抽出と定量的評価等のための基礎データを得ることを進めている。CSMsについては、定性的および定量的な分析を組み合わせた妥当な手法がすでに提案されている。また、今年7月には、ERAから意見を求めるための安全管理システム（SMS）評価基準案がパブリックコメントのために提示された。

以上述べたように、安全を確保するためにはリスク管理によるアプローチが重要である。日本の列車制御・輸送管理システムにおいては、機能安全を中心とするコンピュータ制御の安全性確保のための方策導入に向けて努力が払われてきたが、事故・故障のデータベースの充実や潜在危険源の洗い出しを含め、リスク管理の一層の深度化が必要と考えられる。特に、自動車技術など他分野の新技術導入によって機能向上および低コスト化を実現するうえでも、リスク管理手法の検討が重要となろう。また、鉄道においても、将来、第三者機関によって安全を確認することの議論も必要になろう。安全規格に対して背を向けるのではなく、その適用のメリットに目を向けていくことが大事である。