# 鉄道信号における安全性評価の変遷

平栗　滋人
信号通信技術研究部（信号　研究室長）
ひらぐり　しげと

## はじめに

信号システムは，列車を安全に運行する上で重要な役割を担っています。現在の多くの鉄道では，ある区間単位で，軌道回路によって列車在線を検知し，信号機の現示によって列車に対して安全に走行できる速度を示し，列車同士の間隔を適切に制御しています。さらに，ATS（自動列車停止装置）などによって，停止信号の冒進を防護しています。また，列車進路が分岐，合流する駅構内では，連動装置によって，信号機の現示や分岐器の開通方向が，安全上矛盾の無いように制御されます。さらに，信号システムには，万一，それ自身に故障が発生しても，列車衝突などの危険な事象に至ることが無いような性質を持つことも要求されます。

このような信号システムの役割を実現するための各種の設備やシステムは，当初は経験に基づいて構成されてきた面がありました。これに対して，1970年代半ばに科学的，工学的なアプローチによってシステムの安全性を評価，確保することの必要性が認識され始め，1980年頃にマイクロエレクトロニクス（ME）技術の導入に合わせて，安全性技術の体系化や導入指針の作成が行われました。また，1990年代には，国際規格などの動向も踏まえ，関係者が共通に使用できる技術指針が作成されました。その後，システムの安全性を体系的に評価する技術の重要性がさらに増してきています。

ここでは，このような鉄道信号における安全性の評価に関する動向について紹介します。

## システム安全性工学導入の検討

信号システムには，その発達の過程で装置に故障が発生した場合に，停止信号を現示するなど安全側の状態に遷移するという，フェールセーフの概念が織り込まれてきました。しかし，これを実現する技術は，当初は経験的に開発，導入され，必ずしも体系的に整理されていたとは言えない状況にありました。このような状況に対して，1970年代初め頃から，システム安全性工学を導入して，体系的に信号システムの安全性を確保することの必要性が指摘されました。これを受けて，当時の国鉄において，部外の学識経験者も含めた委員会や部内での検討が行われました。検討は，安全性に関する考え方の明確化，安全性データの蓄積手法の確立，安全性設計手法の体系化，安全性解析手法の確立，安全性管理手法の確立，の各項目について行われました。

この結果，安全性に関する考え方については，機能の維持を目的とする信頼性と，装置故障時にも人命に影響を及ぼすことが無いようにするための安全性とは区別して考える必要があることが指摘されています。また，自動車や航空機など，他の産業分野の調査を行い，安全性技術を，狭義のフェールセーフ（故障時の停止信号現示など），多重化，故障検知と診断などの8つの手法に分類し，これをベースに体系的に整理することを提案しています。

安全性データについては数値的なデータだけでなく，例えば信号システムの回路設計において，具体的な安全上の課題，課題を解決するための対策について，調査，整理が行われました。さらに，この結果を基に安全性設計手法の体系的整理が行われました。

安全性解析手法としては，トップダウン的な手法であるFTA（Fault Tree Analysis）とボトムアップ的な手法であるFMEA（Failure Mode and Effect Analysis）が挙げられています。

また，安全性管理手法については，米軍の安全性管理手法（MIL STD 882A）を参考に検討が行われ，「信号設備安全性管理の手引」（1979年）としてまとめられています。これに示される安全性管理体制の概念を図1に示します。

さらに，この検討が行われた時期には，電子連動装置などME技術を使用した信号システムの開発が行われていました。ここで，電子素子は従来から使用されていた鉄道信

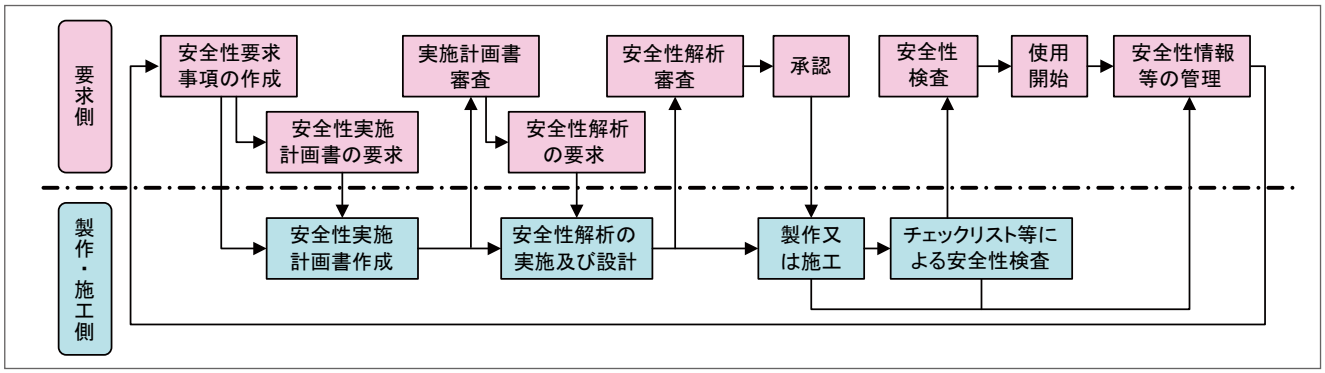


**図１　「信号設備安全性管理の手引」に示される安全性管理体制（抜粋して構成）**

号用リレーとは異なり，故障時の状態を特定することができないため，新しい安全性技術が開発されました。1983年には，これらの成果を反映した「信号保安装置へのマイクロエレクトロニクス導入指針」が当時の国鉄鉄道技術研究所によって作成されました。

## 機能安全の国際規格IEC 61508

ヨーロッパでは，日本と同じように1970年代にORE（当時のUIC（国際鉄道連合）の技術研究所）において，信号システムへのME技術導入に関する検討が始まり，その検討成果が，1990年にUIC Code 738Rとしてまとめられています。この文書では，ME化信号システムのハードウェア，ソフトウェア，情報伝送を対象として，安全性要求仕様の内容，安全性設計技術，システムの認証，プロジェクト管理について述べています。ヨーロッパでは，この他に各国で必要に応じて指針や規格を定めていました。さらに，EU統合に向けて，鉄道信号を対象とする安全性規格を，法的拘束力を持つCENELEC（ヨーロッパ電気標準化会議）規格として作成する検討が進められていました。

一方，IEC（国際電気標準会議）では一般産業分野を対象とした安全性規格の検討に1980年代から着手し，2000年頃にIEC 61508（Part1～Part7）として発行されています。IEC 61508は翻訳されてJIS C0508として，国内でも発行されています。IEC 61508では，概念設計から廃棄までの過程を対象とする「安全性ライフサイクル」と，安全性の要求レベルに応じた技術要件を定める「安全性インテグリティレベル（SIL）」の2つの概念を導入しています。これは，ライフサイクルを厳密に区分，管理することによって，不安全な要素を排除するとともに，要求される安全性のレベルに応じて異なる安全性基準を設定できるようにすることを目的としています。また，潜在する危険そのものを除去する固有安全に対して，ある機能を導入し，潜在する危険のリスクを回避することで安全を実現するという「機能安全」の考え方を導入している点にも特徴があります。なお，「リスク」という用語は，安全に関連する国際規格においては，危険事象の発生確率と，それによる被害の程度の組合せ，と定義されています。

## 列車保安制御システムの安全性技術指針

1980年代半ばの電子連動装置の実用化以降，様々なME化信号装置が導入され，鉄道輸送品質の向上に大きく貢献しました。しかし，先に述べた，「信号保安装置へのマイクロエレクトロニクス導入指針」は，部内資料の性格が強く，広く認知されるには至りませんでした。また，より高度な信号システムの開発に適用可能な，何らかの指針の必要性は認識されていましたが，鉄道事業者，メーカが共通に使用できるものは存在していませんでした。

このような状況や，IEC 61508の検討などの国際的な動向を考慮し，鉄道総研が事務局となって学識経験者，JR，公民鉄，メーカの専門家の参加を得て，「列車保安制御の安全性技術検討委員会」を組織し，1996年に「列車保安制御システムの安全性技術指針」（以下，技術指針と表記）が作成されました。

技術指針はIEC 61508の内容をほぼ包含するとともに，それまでに国内で培ってきた安全要件も取り込む形で作成されています。技術指針は，ヨーロッパの規格とは異なり，体系的な安全性管理に馴染みがなかった国内において，早期に実績を作り，関係者への浸透を図ることが重要であるとの考えから，ガイドラインという位置付けとされました。

技術指針の構成は，本文－解説－資料の3階層となって

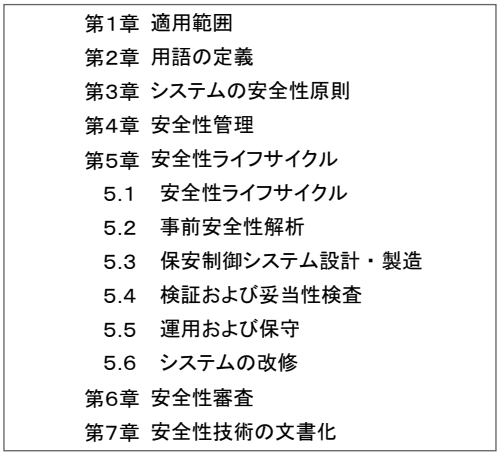


図2　技術指針本文の構成

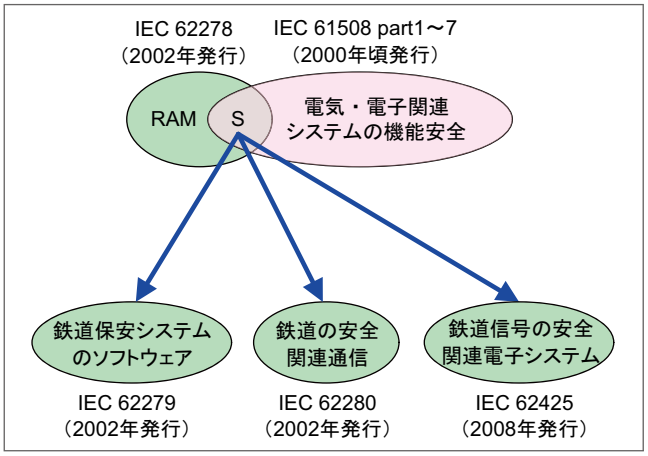


図4　鉄道の安全に関する国際規格の関係

いて，特に解説では技術的要件の背景や考え方に関する説明が述べられています。技術指針本文の構成は，図2に示すようになっています。この内，第5章では，システムの概念設計，事前安全性解析，設計，製造，運用，保守，改修など一連のライフサイクルの各段階（図3）について，その位置付けと要件を記述しています。ここで，実際のシステム設計に入る前の3段階を事前安全性解析段階と位置付け，システムの機能仕様，使用条件，環境条件などの明確化，安全上考慮すべきハザードの抽出とその結果のリスク解析を行い，システムが実現すべき保安機能を明らかにすることを求めています。

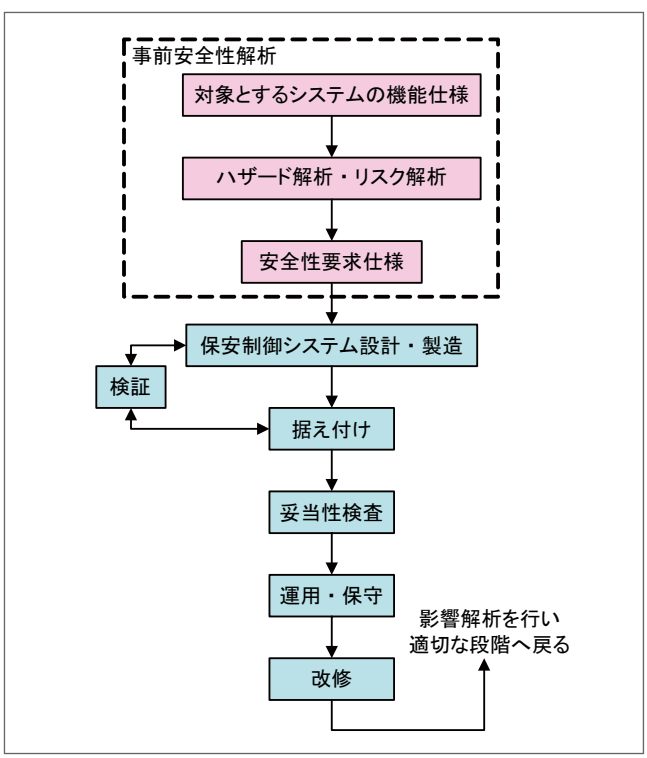


図3　技術指針に示されるシステムライフサイクル

## RAMS規格と関連国際規格

2002年には，鉄道を対象とした国際規格IEC 62278（RAMS規格）が発行されました。RAMS規格は，安全性（S）についてはIEC 61508の考え方をベースとし，これに信頼性（R），アベイラビリティ（A），保全性（M）を加えた4つの指標を経済性と照し合せてバランス良く維持するためのマネジメントシステム規格と位置付けられています。この他に，信号システムを対象とする子規格も国際規格化されています（図4）。この内，IEC 62425では，主にハードウェアを対象として，RAMS規格の考え方に則った上で，信号システムの要件を考慮して，より具体的な内容を規定しています。特にセーフティケースと呼ばれる安全性を証明するための文書群の構成，内容について述べている点が特徴的です。

## 安全性の評価に関する現状

これまでに述べた，1996年の技術指針の作成，あるいはIEC 61508やRAMS規格の発行などの動きが見られるようになって以降，体系的な手法による安全性分析や評価を実施することの重要性や意義が，徐々に認識されるようになり，このような取組みが行われる場合が増えてきたように思われます。特にFTAやFMEAなどの手法によって，事前にハザードを特定し，必要な対策をシステム設計に反映することは，ある程度定着しつつあると言えます。ただし，リスクを指標とする評価や，RAMSの各要素を考慮した総合的なシステム評価については，今後の課題と言えます。

また，国内においては，あくまでも任意ですが，システムの新規開発や，既存システムの改修が発生した場合には，安全性分析の結果を第三者的な組織が評価する事例が多くなってきているようです。

## 安全性分析の実施事例

鉄道総研では，2000年前後に地方交通線向け列車制御システムとして，バリス式列車検知形閉そく装置（COMBAT）の開発を行いました。このシステムは，無線による列車検知方式が従来のシステムとは大きく異なることから，開発時には国際規格への対応を意識して安全性分析を実施しました。

COMBATの開発では，IEC 62425に示されるセーフティケースに対応して事前安全性解析，システム基本仕様，機器仕様，安全性解析，検証試験などに関する各種の文書を作成しました。また，概念設計段階で事前安全性解析を実施し，これを反映した設計書に基づいてFMEA，FTAによる分析，MTBF（平均故障間隔）の算出を行っています。

FMEAでは故障モードの影響分析を行い，装置が誤った制御を行うような故障モードについては，その発生可能性が極めて低いことを示しています。

FTAでは，最終的に列車の衝突，脱線に至る危険事象を解析し，各種診断機能などの安全性技術，および列車検知の無線通信の受信異常に対する処理の有効性を検証した他，危険事象に至る確率が極めて小さいことも試算しています。

MTBFは，システムを構成する装置ごとに算出し，従来の信号システムと同等の計算値を得ています。また，無線による列車検知については他装置の計算値を上回っており，システム全体の弱点とはならないことを確認しています。

## 海外における最近の動向

ヨーロッパでは，欧州鉄道庁（ERA）が鉄道の安全に関するEU指令（Directive 2004/49）に基づいて，共通安全目標（CSTs），共通安全手法（CSMs），共通安全項目（CSIs）の作成作業を進めています。CSTsはリスクの目標値として定義され，受容可能なリスクの評価基準としては，鉄道における個人リスク（旅客，鉄道従事者，踏切，その他）と社会リスクが用いられます。CSMsはCSTsの達成や安全要件の評価方法を示すものです。ここで，示されている手順では，最初にハザードの特定，分類が行われ，鉄道システムに大きな変更があると判断された場合のみ，CSMsが適用されます。また，その際のリスク受容原則として，①既存の規格類，②同様な参照システム，③明示的なリスク評価，の3つが挙げられ，既に使用されている規格類や類似のシステムがあれば，これらの従来の安全確保の方法の適用を認め，これが適当でない場合のみ明示的なリスク評価を行うものです。CSIsは，CSTsの決定や安全レベルを把握し，管理するためのデータとされています。

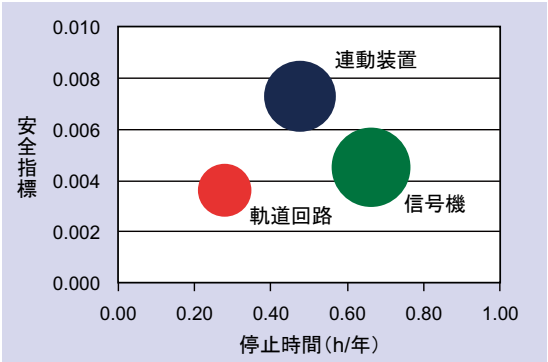


図５　信号システムのリスク試算の例

ヨーロッパにおけるこのような動向や，国際規格の発行により，鉄道における安全に関して，国際的にはリスク管理をベースとする考え方が主流になりつつあると言えます。

## リスク分析手法の検討事例

鉄道総研では，信号システムを対象としたリスク分析手法の検討を行いました。リスクを安全側（列車停止に至るが死傷者を伴わないもの），危険側（死傷者を伴うもの）それぞれの障害の発生確率と，各障害発生時の損害額との積として定義し，モデル線区について試算を行いました。その結果の一例を図５に示します。縦軸の安全指標は，値が大きいほど死傷者の発生する確率が高いことを示している他，装置ごとの円の大きさがリスクを表しています。例えばリスクが最も大きいのは信号機であり，これが優先的に対策を施す必要があることが分ります。また，装置の停止時間，あるいは安全指標に着目し，改善が必要な装置を判断することもできます。つまり，このような手法を適用することによって，鉄道事業者や線区の状況に応じて，効果的な安全対策の適用を支援することが期待されます。

## おわりに

今後は，安全を脅かすハザードの抽出と対策に加えて，リスクやRAMSなどを考慮した総合的な評価方法の重要性が，さらに高まるものと考えられます。このような安全管理の考え方は，ヨーロッパを起源とする部分があり，従来の国内での取組みとは異なる面もあります。しかし，近年，国内でもシステムの安全や，企業の説明責任に対する関心が高まっていることなどを考慮すると，参考にすべき点が多くあることも事実であり，国内でこれまでに培ってきた安全性技術や安全管理の方法を活かした上で，国際的に通用する方法論を確立することが重要と考えられます。RRR